

Meridian Mail Compact Option

System Administration Guide

Publication number:	555-7001-333
Product release:	11
Document release:	Standard 1.0
Date:	November 1997

© 1997
All rights reserved

Printed in Canada

Information is subject to change without notice. Northern Telecom reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

Meridian is a trademark of Northern Telecom.

Publication history

November 1997

Manual released as Standard 1.0. This version of the Meridian Mail Compact Option System Administration Guide is intended for Meridian Mail Compact Option Release 11 base software.

Contents

- | | |
|-----------|---|
| 1 | About this guide |
| 2 | Navigating through system administration |
| 3 | Logging on |
| 4 | Setting up the system |
| 5 | Making voice recordings |
| 6 | Setting up Meridian Mail Compact Option security |
| 7 | User administration—an overview |
| 8 | Local voice users |
| 9 | Remote voice users |
| 10 | Directory entry users |
| 11 | Distribution lists |
| 12 | General administration—an overview |
| 13 | General options |

14	Volume administration
15	Back up and restore Meridian Mail Compact Option data
16	Dialing translations
17	Routine maintenance
18	Voice administration—an overview
19	Voice messaging options
20	Display options
21	Finding and printing VSDNs and service definitions
22	Configuring Meridian Mail Compact Option services
23	The VSDN table
24	Voice services profile
25	Class of Service administration
26	Hardware administration

27	System status and maintenance
28	SEERs and Alarms
29	Operational Measurements
30	Operational Measurements traffic reports
31	User Usage reports
32	Bulk provisioning
A	Integrated Mailbox Administration

Chapter 1

About this guide

In this chapter

<u>Overview</u>	<u>1-2</u>
<u>What this guide is about</u>	<u>1-3</u>
<u>Who should use this guide</u>	<u>1-4</u>
<u>Structure of this guide</u>	<u>1-5</u>
<u>Typographic conventions</u>	<u>1-10</u>
<u>Referenced documents</u>	<u>1-13</u>

Overview

Introduction

This system administration guide provides the procedures and related information necessary to administer a Meridian Mail Compact Option system operating on an Meridian Mail Compact Option platform. This guide includes the initial setup of your system, its daily operation, and its routine maintenance.

Before you begin

All your hardware, including the main administration terminal must already be installed.

What this guide is about

Introduction

This guide explains how to set up, operate, and maintain your Meridian Mail Compact Option system.

Administrative tasks

This guide contains information and procedures for the following:

- setting up the initial system configuration (normally a once-only operation)
- logging on and navigating
- adding users and maintaining the user database
- making voice recordings, such as announcements and voice menus
- setting up system security
- backing up the system
- monitoring system status
- performing routine maintenance
- monitoring traffic reports and system usage reports
- troubleshooting
- configuring special features on your system

Task frequency

Some of these tasks must be performed every day. Others are carried out frequently, while some need to be done only occasionally.

These tasks are performed either through menu-driven screens at your administration terminal or through your telephone.

Who should use this guide

Introduction This guide is intended for users who are responsible for setting up, operating, and maintaining the Meridian Mail Compact Option system.

Guide users There are two main groups of users who refer to this guide:

- The guide's primary users rely on this documentation to do their job.
- The guide's secondary users may need to refer to the documentation to do their jobs.

Examples of users The following table identifies the primary and secondary users of this guide.

Users	Example
Primary users	• database administrators located at customer sites who perform all Meridian Mail Compact Option administration tasks • technical support personnel
Secondary users	• installation and maintenance technicians • database administrators located at customer sites who perform only basic Meridian Mail Compact Option administration tasks • sales engineers • trainers and courseware developers • technical application specialists

Structure of this guide

Introduction

This guide is organized to reflect the hierarchical set of procedures accessible from the Main Menu. Most items that appear in the Main Menu have a corresponding chapter describing the administrative tasks and the screens and fields required to complete the tasks.

Contents of this guide This guide contains the following chapters.

Chapter number and title	Description
Chapter 1: About this guide	Identifies the purpose, scope, audience, and structure of this guide. Sets out the typographic conventions used in the guide. Explains the guide's structure. Lists the publications referred to in this guide.
Chapter 2: Navigating through system administration	Provides an overview of the functional areas presented in the System Administration menu. Describes basic screen navigation tools and techniques. Introduces the Meridian Mail Compact Option user interface. Lists the features available for each Meridian Mail Compact Option hardware platform and user interface.
Chapter 3: Logging on	Describes how to log on to Meridian Mail Compact Option. Describes how to log on to the Option11C Compact through a Meridian Mail Compact Option administration terminal.
Chapter 4: Setting up the system	Refers users to procedures for checking the provisioning of Meridian Mail Compact Option. Provides an overview of a complete basic setup of Meridian Mail Compact Option, with cross-references to relevant information and procedures in other chapters and guides.
Chapter 5: Making voice recordings	Describes how to make voice recordings for use by Meridian Mail Compact Option.

Chapter number and title	Description
Chapter 6: Setting up Meridian Mail Compact Option security	Identifies the high-risk areas of a Meridian Mail Compact Option system and the types of abuse that can occur. Lists the measures that can be taken to set up and monitor system security. Describes the use of security features to prevent unauthorized mailbox access. Describes measures to prevent the use of Meridian Mail Compact Option features for unauthorized long distance calling. Suggests procedures to prevent unauthorized use of the administration terminal. Describes the reporting features available to help administrators detect abuse.
Chapter 7: User administration — an overview	Introduces the concepts and issues concerning user administration. Cross-references appropriate chapters for routine user administration tasks of particular interest or concern.
Chapter 8: Local voice users	Describes procedures for administering local voice users.
Chapter 9: Remote voice users	Describes procedures for administering remote voice users.
Chapter 10: Directory entry users	Describes procedures for administering directory entry users.
Chapter 11: Distribution lists	Describes procedures for administering system distribution lists.
Chapter 12: General administration — an overview	Introduces the concepts and issues concerning general administration. Directs users to the appropriate chapters for routine general administration tasks.
Chapter 13: General Options	Describes how to perform the tasks and locate the information available under the General Options screen.

Chapter number and title	Description
Chapter 14: Volume administration	Describes the tasks that can be performed through the volume administration side of Volume and selective backups.
Chapter 15: Back up and restore Meridian Mail Compact Option data	Explains the importance of Meridian Mail Compact Option system backups. Suggests which volumes to back up, and how frequently. Describes the two available backup media and how to perform a backup with either one. Describes the procedures for scheduling a backup to occur automatically at a later time and for checking on the status of a backup in progress.
Chapter 16: Dialing translations	Introduces the concept of dialing translations. Specifies the situations and features requiring dialing translations. Guides users through setting up dialing prefixes and translation tables appropriate to their system. Provides in-depth detail for those who wish to customize dialing translations.
Chapter 17: Routine maintenance	Lists the routine maintenance tasks recommended for optimum Meridian Mail Compact Option operation.
Chapter 18: Voice administration—an overview	Provides an overview of voice administration. Describes the Voice Administration menu and its menu options. Directs users to the appropriate chapters for documentation of the menus and screens accessible from the Voice Administration menu.
Chapter 19: Voice messaging options	Describes the tasks that can be performed using the Voice Messaging Options screen.
Chapter 20: Display options	Describes how to change the display options for the Voice Services Administration screen using the Set Display Options screen.

Chapter number and title	Description
Chapter 21: Finding and printing VSDNs and service definitions	Describes how to use the Find function to find and print VSDNs and service definitions.
Chapter 22: Configuring Meridian Mail Compact Option services	Provides an overview of the configuration of Meridian Mail Compact Option services: the setup of the Option 11C Compact and Meridian Mail Compact Option setup.
Chapter 23: The VSDN table	Documents the procedures for configuring VSDNs for each Meridian Mail Compact Option feature that potentially requires a DN.
Chapter 24: The voice services profile	Documents the tasks that can be performed using the Voice Services Profile screen. Provides information about the different kinds of timeouts and how they work.
Chapter 25: Class of Service administration	Introduces the concept of Class of Service and the types of Class of Service. Guides users through creating, assigning, changing, and deleting individual Classes of Service.
Chapter 26: Hardware administration	Describes the methods for viewing and printing out the configuration of Meridian Mail Compact Option's dedicated nodes and data ports.
Chapter 27: System status and maintenance	Describes procedures for checking on system, card, and port status. Describes procedures for enabling and disabling certain system components as part of routine maintenance, troubleshooting, and replacement. Describes the use of the Channel Allocation Table during system expansion or reorganization.

Chapter number and title	Description
Chapter 28: SEERs and Alarms	Introduces the concepts of SEERs and alarms. Describes how to customize a system's SEER processing protocols to control how certain SEER messages are categorized and reported.
Chapter 29: Operational Measurements	Provides an overview of the Operational Measurements feature and how it can be used to monitor Meridian Mail Compact Option system activity. Describes how to generate, view, print, and analyze Operational Measurement reports.
Chapter 30: Operational Measurements traffic reports	Provides information and procedures for Operational Measurements traffic reports.
Chapter 31: User Usage reports	Provides information and procedures for Operational Measurements user usage reports.
Chapter 32: Bulk provisioning	Introduces the concept of bulk provisioning. Offers examples of situations where bulk provisioning can be used. Describes procedures for transferring bulk provisioning data onto tape and into another Meridian Mail Compact Option system.
Appendix A: Integrated Mailbox Administration	Presents information and procedures for avoiding data corruption or task conflicts when using the Integrated Mailbox Administration feature to administer mailboxes.

Typographic conventions

Introduction

This topic describes the typographic conventions used in this guide for the following:

- softkeys
- keyboard keys or hardkeys
- telephone keypad keys
- text input
- fields in a menu
- values in a field
- system responses
- spoken words
- recorded prompts

Conventions

The following table identifies, describes, and provides examples of the conventions used in this guide.

Convention for	Description	Example
softkey	Softkeys are displayed on the administration menus and screens. They indicate which keyboard function keys you press to carry out specific Meridian Mail Compact Option tasks. A softkey is referred to by its label (as displayed in the menu or screen) enclosed in square brackets. It appears in the same typeface as the accompanying text.	[Exit] [Record]

Convention for	Description	Example
keyboard key or hardkey	A keyboard key or hardkey is referred to by its label enclosed in angle brackets. When two key names appear together, you press them both at the same time. A keyboard key or hardkey appears in the same typeface as the accompanying text.	<1> <Prev Screen> <Help> <Return> <Ctrl> <r>
telephone keypad key	The telephone keypad keys that you press appear in bold print in the same typeface as the accompanying text.	Press 829 on the telephone keypad.
text input	Text that you type appears in bold print. In a procedure, it appears in the same typeface as the accompanying text. In other text, it appears in a different typeface from the accompanying text.	Type m .
fields in a menu	The name of a field is capitalized and appears in the same typeface as the accompanying text.	the Last Name field the Invalid Logon Attempt field
values in a field	A value in a field is capitalized and appears in the same typeface as the accompanying text.	The default is No.
system responses	System responses appear in the same typeface as the accompanying text. They are often introduced with Result: .	Result: <i>The system prompts you for a password.</i>
spoken words	The suggested wording of a greeting or an announcement appears in italics enclosed in double quotation marks.	You might want to include the following statement in your voice menu: <i>"Please wait on the line. An Attendant will be with you shortly."</i>

Convention for	Description	Example
recorded prompts	Prompts played by the system appear in italics enclosed in double quotation marks (the same as spoken words).	<i>"You have no new voice messages. One old message is still unsent."</i>

Cross-references

For a cross-reference to another part of this guide or to another manual, the following conventions are used.

Cross-reference	Convention	Example
to another topic in this guide	This cross-reference is enclosed in double quotation marks.	For more information, <u>see</u> "Logging in to Meridian Mail Compact Option" on page 5-9.
to another manual	The title of the manual appears in italics. The applicable reference number is also presented.	Refer to the Meridian Mail System Administration Tools Guide (NTP 555-7001-305).

Referenced documents

Introduction

You may find it useful to have a number of additional resources available as you are reading this manual.

Referenced documents

The following table identifies the documents that are referred to in this guide.

NTP number	Title	Description
555-7001-305	Meridian Mail System Administration Tools	Documents additional administrative tools and utilities that are available at the tools level.
555-7001-510	<i>Maintenance Messages (SEERs) Reference Manual</i>	Lists System Event and Error Reports (SEERs) to help isolate and fix system problems.
553-3001-300	<i>Meridian 1 X11 System Management Overview, Applications, and Security</i>	Provides an introduction to the system management facilities provided with the Meridian 1 switch.

Chapter 2

Navigating through system administration

In this chapter

<u>Overview</u>	<u>2-2</u>
<u>Section A: The administration menu hierarchy</u>	<u>2-3</u>
<u>Section B: Understanding menus, screens, and keys</u>	<u>2-19</u>
<u>Section C: Meridian Mail Compact Option features and interface</u>	<u>2-39</u>

Overview

Introduction

This chapter contains the following information:

- an overview of how the menus are arranged into a hierarchy
- an overview of the functional areas presented in the Main menu
- the layout of screens and menus
- navigation tools and techniques
- instructions on how to modify fields
- a list of the features available for the MMUI on the Meridian Mail Compact Option platform

Section A **The administration menu hierarchy**

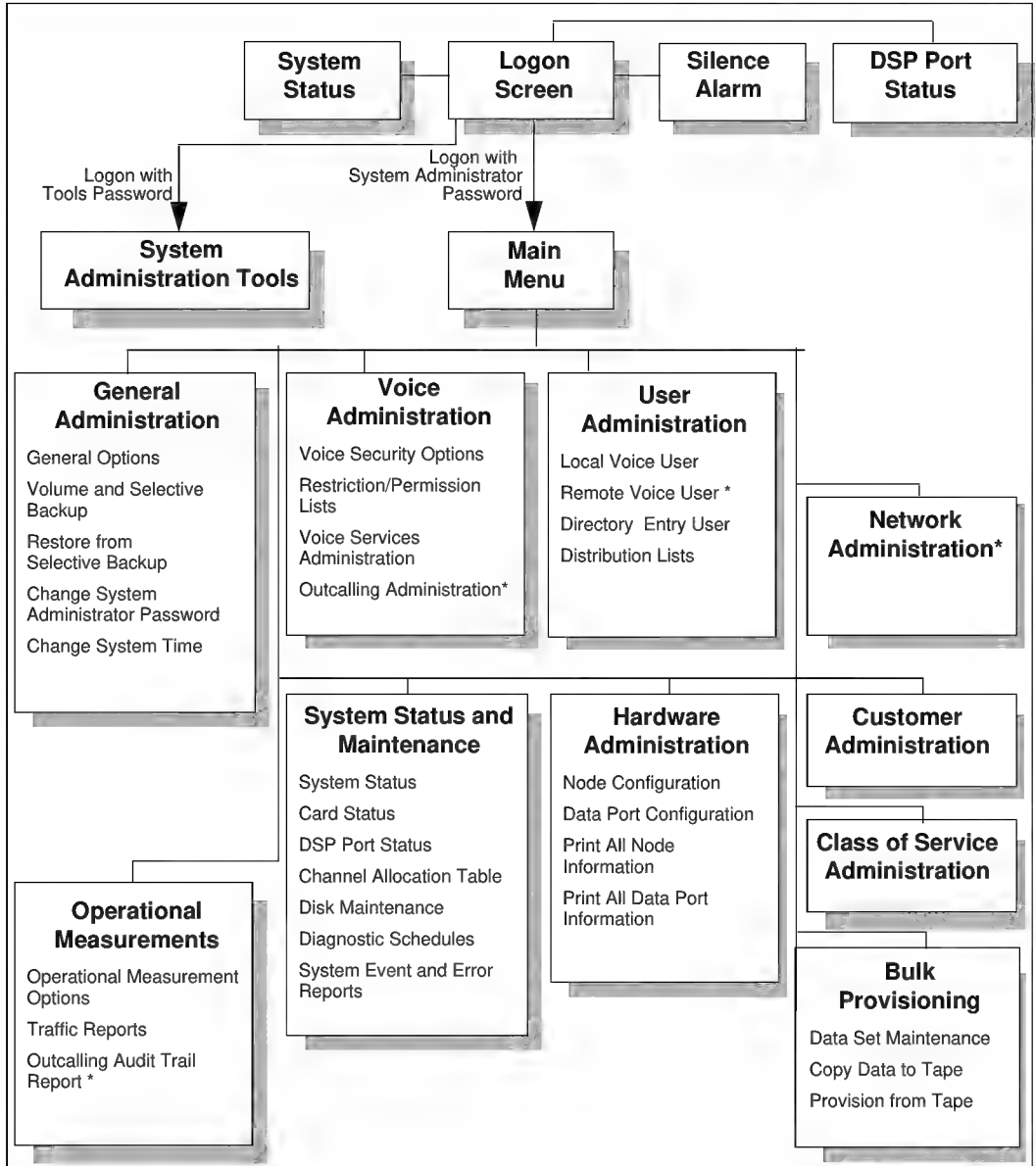
In this section

<u>The Main menu</u>	<u>2-6</u>
<u>User administration</u>	<u>2-7</u>
<u>General administration</u>	<u>2-8</u>
<u>Voice administration</u>	<u>2-9</u>
<u>Hardware administration</u>	<u>2-12</u>
<u>System status and maintenance</u>	<u>2-13</u>
<u>Operational measurements</u>	<u>2-16</u>
<u>Class of Service administration</u>	<u>2-17</u>
<u>Network administration</u>	<u>2-18</u>

The system administration menu hierarchy

Menu hierarchy

The following is an example of the system administration menu hierarchy.



* Available only if the necessary feature is installed.

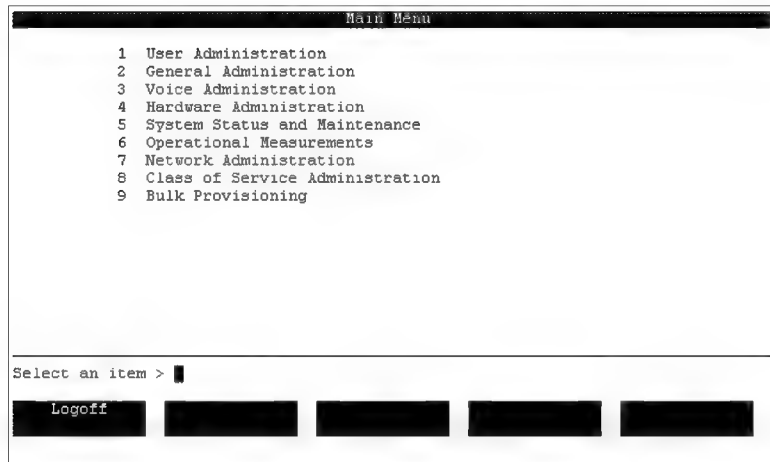
The Main menu

Introduction

The Main menu is the first screen that is displayed after you log on. This menu is your starting point for performing Meridian Mail administration tasks.

The menu

Here is an example of the Main menu.



Feature-dependent items

The following menu items are displayed only if the appropriate feature is installed:

- Network Administration is displayed if Meridian Mail Networking is installed.

User administration

Description	User administration involves creating and maintaining a database of users.
Local voice users	Local voice users have mailboxes. You can add, modify, and delete local voice users in User Administration. You can also carry out other user-related functions such as recording personal verifications.
Remote voice users	If Enterprise Networking is installed, you can add users at remote sites to your local user database. One way of adding and deleting remote voice users is through User Administration. Remote voice users can be added to distribution lists at the local site. Local users can use name dialing and call sender to call remote voice users and name addressing to compose messages to them.
Directory entry users	Directory entry users do not have mailboxes. They are, however, in the user directory, and therefore can be accessed by features such as name dialing and Thru-Dial. These users are added, modified, and deleted from User Administration.
Distribution lists	Distribution lists contain a list of mailbox numbers. Whenever you send a message to a distribution list, it is sent to all of the mailboxes in the list. Administering distribution lists involves • assigning a number to each list • adding mailbox numbers to each list • keeping the lists up to date • recording a personal verification for each list

General administration

Introduction

General Administration is divided into a number of administration areas from which you can perform a variety of tasks.

Defining general options

Defining general system options involves the following tasks:

- assigning classes of service to the system
- defining the attendant DN
- setting the date format for reports
- specifying the SEER printer and Reports printer port names

Backing up and restoring data

You can perform the following types of backups:

- volume backups (of data and voice) to tape
- selective backups (of data only) to tape selective backups of users or services to tape

From Generation Administration, you can restore only users or services that were selectively backed up.

For information about restoring data from selective backup, see “Restoring information from a Selective backup” on page 15-45.

Changing passwords and the system time

You can change the following:

- the system administrator password
- the system time

Voice administration

Introduction

Voice Administration is divided into a number of administration areas from which you can perform a variety of tasks.

Defining voice messaging options

Defining voice messaging options involves the following tasks:

- If more than one language is installed, you must define the default language and whether it overrides users' preferred languages.
- If Dual Language Prompting is installed, you must define the secondary language in which prompts are played.
- You can record customized versions of the call answering greeting MMUI tutorials.
- You can enable or disable name dialing/name addressing and external call sender.
- You can define operational characteristics for voice messaging such as
 - the maximum delay for timed delivery
 - the broadcast mailbox number
 - the maximum number of days that read messages are retained

Defining voice security options

Defining voice security options is extremely important in order to safeguard your system from unauthorized use and abuse by hackers and users. You can do the following to secure your Meridian Mail Compact Option system:

- Make mailbox passwords more secure by
 - defining the password prefix
 - specifying the minimum password length
 - forcing users to change their passwords the first time they log on
 - suppressing the display of passwords on the telset
- Specify the maximum number of invalid logon attempts that are allowed before a mailbox is disabled or a session terminated.
- Set up monitoring periods for
 - system accesses
 - thru-dials
 - specific internal or external, or both, calling line IDs (CLIDs)

Defining restriction/permission lists

Restriction/permission lists are another very important part of ensuring system security. A restriction/permission list specifies which dialing codes are not allowed, thereby preventing users or callers from placing calls to unauthorized numbers such as domestic long distance numbers or international numbers.

You can define up to 80 different restriction/permission lists that can then be applied to different features that place outcalls such as call sender, and Thru-Dial.

Performing voice services administration

Voice Services Administration is divided into a number of administration areas.

- The VSDN Table is where you add voice service DN's (VSDNs) for each service that you want to make directly dialable by a unique number.
- The Voice Services Profile is where you define characteristics for voice services such as timeouts and holidays (used by time-of-day controllers)
- You can add, modify, and delete the following voice services from Voice Services Administration:
 - announcement definitions
 - thru-dial definitions
 - time-of-day controller definitions
 - voice menu definitions

Setting display options

Display options allow you to choose

- how you want information sorted in Voice Services Administration screens
- whether or not the Choice of Services and Menu Actions lists are displayed

Hardware administration

- Introduction** Almost all of the screens in Hardware Administration are read-only. They are for viewing purposes only.
- To modify your hardware configuration, you must log on to the Tools level and access the Modify Hardware tool. For more information, refer to *Meridian Mail System Administration Tools* (NTP 555-7001-305).
- Node configuration** You can view the number of nodes that are installed and the types of cards that have been configured for each node.
- Data port configuration** You can view configurations for the following data ports:
- Terminal
 - Printer
 - Diagnostics
- Printing information** You can print all node and all data port information.

System status and maintenance

Introduction

System Status and Maintenance primarily involves viewing the status of the system and various hardware components to see if everything is operational.

When a hardware component needs servicing, it must first be disabled and then reenabled when the problem is fixed. This is done in System Status and Maintenance.

Viewing status and disabling components

For each of the following hardware components, you can view its status, disable (or courtesy disable) it for servicing, and reenable it:

- the entire system
- cards
- DSP ports

Channel Allocation Table

The Channel Allocation Table shows how channels (ports) are allocated to services.

From the Channel Allocation Table, you can view the following:

- the channels that are on your system, their type, and whether they are shared by services or dedicated to a particular service for placing outbound calls
- the maximum number of each type of port, and how many of each port type have been allocated

**The Channel
Allocation Table cont'd**

If you disable ports, you can do the following:

- Modify the Primary DN.
- Modify Channel DN.
- Modify the capability.

Disk maintenance

Unshadowed systems

On unshadowed systems, you can view the status of the prime disk and perform diagnostics.

Diagnostic schedules

You can schedule diagnostics to occur at a specific time on certain days. You can specify the following about the scheduled diagnostics:

- whether voice path diagnostics should be performed, and other related parameters

**System event and
error reports**

You can perform the following tasks from the System Event and Error Reports menu.

SEER retrieval

If you do not want all SEERs to be retrieved, you can specify which SEERs should be retrieved according to SEER class, severity level, or SEER type.

SEER configuration

From the SEER Configuration screen, you can do the following:

- Specify the mailbox (the message trigger mailbox) to which you want messages to be sent when a SEER that meets a specific criteria is generated. This allows you to be notified immediately of SEERs that you consider to be critical.
- Set SEER throttling parameters which allow you to prevent SEERs that are duplicated a certain number of

times from being sent to the printer or message trigger mailbox, or both.

- Set SEER escalation parameters which allow you to specify how many times a SEER needs to be duplicated before it is escalated to the next severity level.
- Set the SEER filtering levels which allow you to control which SEERs are sent to the printer and message trigger mailbox (according to type and severity level).

SEER remapping

SEER remapping allows you to remap the severity level of up to 60 SEERs to a different severity level and have that information stored on disk.

For example, a SEER that is classified as major in Meridian Mail Compact Option may be critical to your particular system. You could, therefore, remap this SEER as critical.

Operational measurements

Introduction

There are two kinds of operational measurement reports: traffic reports and user usage reports.

Operational measurement options

Setting operational measurement options involves specifying

- whether to collect traffic, user usage, session trace, the start and end times for the traffic period
- the number of days traffic data and user usage data are stored

Traffic reports

You can view or print a summary of traffic report services that shows the number of accesses, the average length, and voice mail usage.

You can view or print more detailed traffic reports for the following:

- Voice Messaging
- Channel Usage
- Services
- Networking
- Disk Usage

User usage reports

You can view or print user usage reports which provide local usage data and Enterprise Network usage data.

Class of Service administration

Introduction

Before you can add local voice users, you must create your classes of service (COS). Each local voice user must be assigned to an already defined class of service.

COS-controlled features

Classes of service determine the feature capabilities of the local voice users assigned to them. Some examples of features and limits that are controlled by classes of service are

- the voice storage limit
- the maximum length of composed messages
- the maximum length of call answering messages
- the ability to send broadcast messages
- notification of busy line to callers

Maintaining classes of service

Maintaining classes of service involves modifying classes of service as needed. Whenever a change is made to a class of service, the change is propagated to all users belonging to that class of service.

It also involves deleting classes of service that are no longer needed (and reassigning users to another class of service before you delete).

Network administration

Description Network administration involves the administration of Enterprise Networking.

Enterprise Networking Administration of the Enterprise Networking features involves

- local site maintenance
- remote site maintenance, which involves adding remote sites, specifying the Enterprise Networking protocol and dialing plan for each site, and recording a spoken site name
- network configuration, which involves setting initiation times, holding times, stale times, the batch threshold, and wakeup interval
- checking the network status periodically

Section B **Understanding menus, screens, and keys**

In this section

<u>Overview</u>	<u>2-20</u>
<u>Keypad functions</u>	<u>2-21</u>
<u>Meridian Mail Compact Option menus</u>	<u>2-23</u>
<u>Meridian Mail Compact Option screens</u>	<u>2-25</u>
<u>Getting around in screens</u>	<u>2-28</u>
<u>Entering information in fields</u>	<u>2-30</u>
<u>Softkeys</u>	<u>2-35</u>
<u>Getting help</u>	<u>2-37</u>
<u>Error messages</u>	<u>2-38</u>

Overview

Introduction System administration menus and screens have a consistent format. The way in which items are selected and data is entered is the same for all menus and screens.

In this section This section describes

- keypad functions
- the layout of menus
- the layout of screens
- types of fields
- how to select menu items
- how to select options and enter data in fields
- how to navigate through fields in screens
- how to scroll through multipage screens
- softkeys
- how to get help

Keypad functions

Application mode	When the keypad is in application mode, certain functions are available on the keypad when you press single keys or key combinations. Application mode is the default whenever the system is rebooted.
Supported terminals	Keypad functions are supported on VT220 terminals and the following VT200-compatible terminals: VT320, VT420, HP700/22, and HP700/32.
Numeric keypad	If you choose to work with a numeric keypad (where the numeric keys generate numbers when you press them), then only the F1, F2, F3, and F4 keys retain the functions indicated. The keypad is set to numeric mode through the terminal's setup function.
Keypad function key positions	The following illustration shows the functions available when the keypad is in application mode.

F1	F2	F3	F4
7	8	9	—
4	5	6	,
1	2	3	
0		.	ENTER

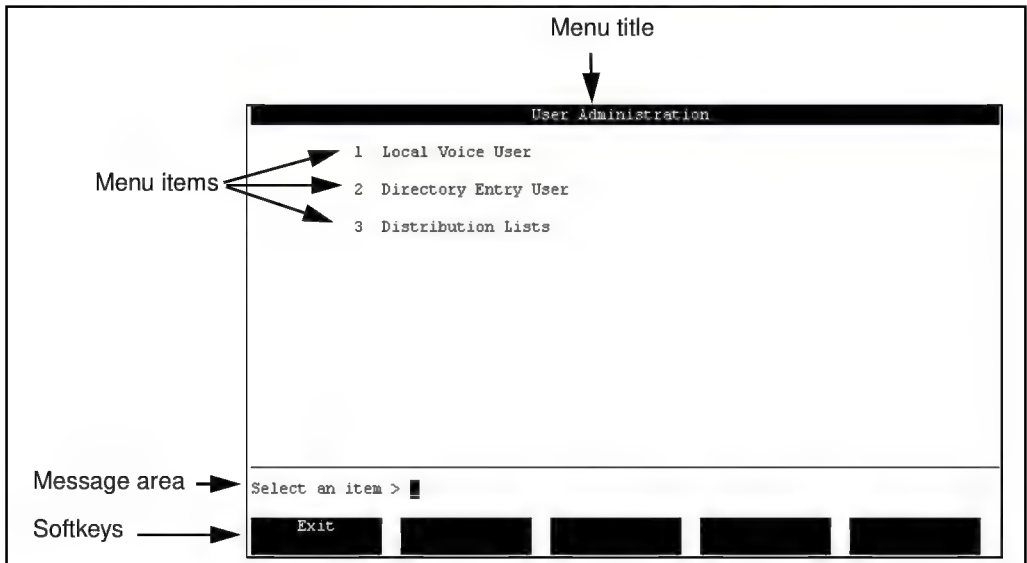
F1 - Softkey 1
 F2 - Softkey 2
 F3 - Softkey 3
 F4 - Softkey 4
 1 - Start of field
 2 - Next word in field
 3 - End of field
 4 - Previous field
 5 - Next field
 7 - Previous page
 8 - Next page
 - - Delete field contents
 . - HELP
 ENTER - Softkey 5

(shading indicates that the key does not have a function)

Meridian Mail Compact Option menus

Description A menu presents a list of items from which you can choose. When an item is selected, either another menu or a screen is displayed.

A typical menu The following is an example of a menu.



Parts of a menu This table describes the parts of a menu.

Part	Description
Menu title	Menu titles are always on the first line.
Menu items	Each menu has a list of choices that are preceded by numbers. These are menu items from which you can choose. Choosing a menu item causes either another menu or a screen to be displayed.

Part	Description
Message area	This is where system prompts, responses, and error messages are displayed.
Softkeys	The bottom line in a menu is a set of softkeys. Softkeys are used to carry out actions.

Choosing a menu item Each item in a menu has a number. The system displays a prompt requesting you to make a selection from the items presented.

To select a menu item, follow these steps.

Starting Point: Any menu with the “Select an item” prompt displayed

Step Action

- 1 Enter the number that corresponds to the item you want to choose and press <Return>.

Example: You want to add local voice users to your system so you enter 1 and press <Return>.

```

User Administration

1 Local Voice User
2 Directory Entry User
3 Distribution Lists

Select an item >|
Exit [ ] [ ] [ ] [ ]

```

Result: Another menu or a screen is displayed.

Meridian Mail Compact Option screens

Description	Screens contain fields in which you can either make selections or enter data. It is by filling in fields that you customize Mail to meet your requirements and suit your needs.
A typical screen	The following is an example of a screen.

The diagram illustrates a system administration screen titled "Add Class of Service" under the menu "Class of Service Administration". The screen is annotated with labels and arrows indicating various navigation elements:

- Menu title:** Points to the top bar "Class of Service Administration".
- Screen title:** Points to the main heading "Add Class of Service".
- Fields:** A bracket on the left groups the following input fields:
 - Class of Service Number: 7
 - Class of Service Name: Marketing
 - Personal Verification Changeable by User: No Yes
 - Voice Storage Limit (minutes): 3
 - Maximum Message Length (mm:ss): 03:00
 - Delayed Prompts: No Yes
 - Auto Logon: No Yes
 - Administrator Capability: No Yes
- Message area:** Points to the text "Select a softkey >" below the first set of fields.
- Softkeys:** Points to the row of buttons: Save, Cancel, and three unlabeled buttons.
- More below indicator:** Points to a button labeled "MORE BELOW" on the right side of the first section.
- More above indicator:** Points to a button labeled "MORE ABOVE" on the right side of the second section.
- Fields (Second Section):** A bracket on the left groups the following input fields:
 - External Call-Sender Receive Composed Messages: No Yes
 - Message Waiting Indication Options: None Any Urgent
 - External Call-Sender Message Waiting Indication Options: None Any Urgent
 - External Call-Sender Class of Service Number: 7
 - Class of Service Name: Marketing
 - Personal Verification Changeable by User: No Yes
- Message area (Second Section):** Points to the text "Select a softkey >" below the second set of fields.
- Softkeys (Second Section):** Points to the row of buttons: Save, Cancel, and three unlabeled buttons.

Parts of a screen

This table describes the parts of a screen.

Part	Description
Menu title	This is the name of the menu from which the screen was accessed.
Screen title	The name of the screen.
Fields	Fields in screens are much like fields in forms. You can either enter information in them, or select from a predetermined set of options. It is by filling in fields that you define how you want Meridian Mail Compact Option to work and customize the system to meet your needs.
Message area	This is where system prompts, responses, and error messages are displayed.
Softkeys	The bottom line in a menu is a set of softkeys. Softkeys are used to carry out actions.
More below indicator	This indicator is displayed in multipage screens. It indicates that there are more fields below the last field that is currently displayed.
More above indicator	This indicator is displayed in multipage screens. It indicates that there are more fields above the first field that is currently displayed.

Getting around in screens

Navigating between fields

The following keys on the keyboard and on the application keypad ([see “Keypad functions” on page 2-21](#)) move the cursor between fields.

IF you want to	THEN press
move to the next field	• the Tab key • the down arrow key • the Return key, or • 5 on the application keypad.
move to the previous field	• the up arrow key, or • 4 on the application keypad.

Moving through multipage screens

Certain screens contain more fields than can be displayed at one time on the display terminal. You can view additional pages in one of two ways: by scrolling and by paging.

Scrolling

If you see “More Below” at the bottom of a screen or “More Above” at the top of a screen, you can use the following keys.

IF you want to	THEN press the
view the next page of a multipage screen	• Next Scrn hardkey.
view the previous page of a multipage screen	• Prev Scrn hardkey.

When the “More Below” prompt disappears, you are at the end of the screen. When the “More Above” prompt disappears, you are at the top of the screen.

- Using the down arrow key** The down arrow key displays only the last input field, even if there is instructional text below it. To view any text that may appear at the end of a screen, use the Next Scrn hardkey.

- Paging** In some screens, a [Next Page] softkey is displayed that can be used to move between the pages of a screen.

Entering information in fields

- Introduction**
- Information is entered in the fields of Meridian Mail Compact Option screens. There are two types of fields:
- selectable fields
 - data entry fields

Example

This screen contains both types of fields.

Selectable fields

Data entry fields

Selectable fields

User Administration

MORE ABOVE

View Class of Service

Receive Composed Messages: No **Yes**

Message Waiting Indication Options: None **Any** Urgent

External Call-Sender

Restriction/Permission List: 2 List Name: Local

Read Message Retention (days): 0

("0" implies that read messages are retained until the user deletes them manually.)

Send Messages to External Users: **No** Yes

Retain Copy of Sent Messages: **No** Yes

MORE BELOW

The Class of Service data will be saved only if the user is saved.

Return to Basic Fields

Selectable fields

Selectable fields present a number of predefined options from which you can choose.

The option that is in reverse video (light text on a dark background) is the selected option.

After installation, selectable fields always have one of the options selected as the default.

Examples

Examples of selectable fields in the above screen example are Receive Composed Messages and Retain Copy of Sent Messages.

Choosing an option in a selectable field

To choose a predefined option in a selectable field, follow these steps.

Step Action

- 1 Move the cursor to the field you want to modify.
- 2 Use the right (and left) arrow keys, or the spacebar, to select the option you desire.

Note: The selected option appears in reverse video.

Data entry fields

You type information, such as titles and numbers, into data entry forms. There are often limitations placed on data entry fields, such as the types of characters you can enter or a range of numbers. Data entry fields are indicated by an underline next to the field name. This is where you enter information.

Some of these fields are prefilled with default values. These values can be changed as needed. Others are blank by default and require an entry.

Example

An example of a data entry field (on page [2-30](#)) is the Read Message Retention (days) field.

Entering information in a data entry field

To enter information in a data entry field, follow these steps.

Step Action

- 1 Move the cursor to the field you want to modify.
- 2 Is there currently any information in the field?
 - If yes, [go to step 3](#).
 - If no, [go to step 4](#).
- 3 Delete the current content of the field.

IF you want to	THEN press
clear the current contents	the <Remove> key.
delete one character to the left of the cursor	the <x> key.
delete the character on which the cursor is positioned	the <Back Space> key.

- 4 Type the information in the field.
-

Selecting an entire line

In some screens, especially those that provide a list of things from which to choose, you need to select an entire line to indicate on which item you want to perform an action, and then press a softkey to indicate which action you want to perform.

To select an entire line in a screen, follow these steps.

Step Action

- 1 Move the cursor to the line you want to select using the up and down arrow keys.
 - 2 Press the spacebar.
Result: The entire line is selected (as indicated by reverse video).
-

Prompt

Screens requiring this mode of selection often indicate this with the following prompt: “Move the cursor to the item and press the spacebar to select it.”

Example

You want to record a personal verification for all users assigned to class of service 2 that do not currently have personal verifications.

After using Find, you get this list of users. You select the first user, Bob LePage, and then press [Voice] to record the personal verification.

User Administration						
List of Local Voice Users						
Name	Mailbox	Department	COS Num.	Storage Used (mins)	Personal Verific. Recorded	
LePage, Bob	65551234	9t23	0	0	No	
Rorty, Phillip	65558050	9t23	0	0	No	
Select a softkey >						
Exit	Toggle Cos Assignment	View/Modify	Delete	Voice		

Mandatory fields

Certain data fields require you to insert values, whereas other fields are optional. Mandatory fields are identified in the field descriptions.

If you do not fill in a mandatory field and then try to save your settings, the system does not save the screen but, instead, prompts you to fill in the necessary field.

Softkeys

Description

Softkeys appear on the bottom two lines of menus and screens and are displayed in reverse video (light characters on a dark background).

They correspond to function keys F1 through F5 or F6 through F10 on the top row of the keyboard. The softkeys change according to the menu or screen. They may also change with the function you are performing.

Purpose

Softkeys are always actions. When you select a softkey, you are performing a function.

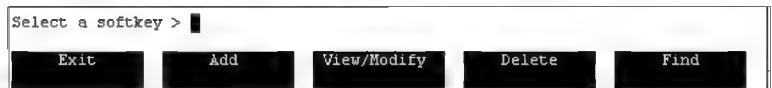
Common softkeys

The following softkeys occur on the administration screens:

- [Exit]
- [Add]
- [View/Modify]
- [Delete]
- [Find]
- [Save]
- [Cancel]

Softkey positions

If any of these keys occur on a screen, they typically occur in the following positions.



Select a softkey >				
Save	Cancel			

Getting help

Introduction

Online help is available for most of the menus and screens, including the Main Menu.

Procedure

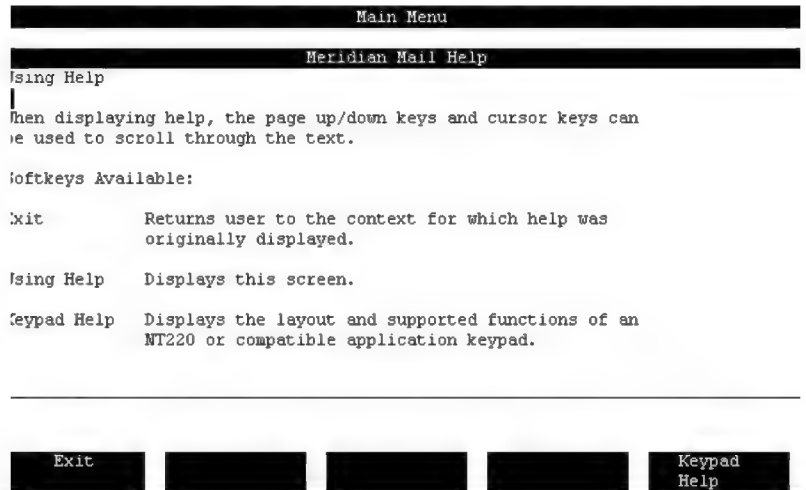
To get Help, follow these steps.

Step Action

- 1 Press the Help key.
Result: The system displays explanations of the fields on the menu or screen in which you are working.
- 2 Once you are done reading the Help information, press the [Exit] softkey to return to the menu or screen.

A typical Help screen

The following shows an example of a Help screen.



Error messages

Introduction

The system displays error messages, both general and screen-specific, on the line above the softkey display.

These messages remain on the screen until the next user input or until another error message appears.

Purpose

These messages provide feedback on administration actions. They should not be confused with System Event and Error Report (SEER) messages.

SEER messages

If SEER printing is disabled, SEER messages will print out on the administration screen.

Examples of error messages

The following are two examples of error messages:

- “The key entered is not valid at this time.”
- “Enter a number in the range of 1 to 6.”

Section C **Meridian Mail Compact Option features and interface**

In this section

[The main administration terminal](#) [2-40](#)

[Meridian Mail Compact Option telset interface](#) [2-41](#)

The main administration terminal

Introduction

Meridian Mail Compact Option is administered through a menu-driven administration interface available at a terminal or personal computer (PC) using terminal emulation software. Using the administration menus, you establish the initial configuration of your system, maintain the user information base, create voice applications such as announcements and voice menus, monitor system usage and performance, and perform routine system maintenance.

The main administration terminal

All of these tasks are performed from the main administration terminal or from a PC using terminal emulation software.

Meridian Mail Compact Option telset interface

Introduction Through the Meridian Mail Compact Option telset interfaces, which is a Meridian Mail user interface (MMUI), users interact with the system to log in to their mailboxes, listen to messages, and compose and send messages.

Definition: MMUI The MMUI interface is a full-featured command-driven Northern Telecom (Nortel) proprietary voice mail interface.

Terminology: users Users added to a system on which the MMUI interface is installed are referred to as *users*.

Available features This table indicates which features are available for the Meridian Mail user interface

Feature	MMUI
handling of forwarded calls	yes
personalized greetings	yes
message waiting indication (MWI) support	yes
password-protected mailboxes	yes
mailbox summaries and message playback	yes
message reply, reply all, and message forward	yes
personal distribution lists	yes
message compose and send	yes
Enterprise Networking	yes
ability to assign a class of service (COS)	yes
18-digit mailbox	yes

Feature	MMUI
mailbox Thru-Dial (A user can press 0 and dial a number while logged in to the mailbox.)	yes
name addressing (A user can dial another user by name instead of by extension.)	yes
message tagging options (During message composition, a user can tag messages as urgent or for timed delivery.)	yes
retention of sent or unsent messages	yes
internal, external, and temporary greeting	yes
user-changeable personal verification	yes
customizable customer greeting and customer attendant	yes
custom operator revert	yes
user-changeable remote notification schedules through the telephone set	yes
express messaging	yes
bilingual prompting (if more than one language is installed)	yes
record, playback, and message tagging during call answering	yes
adding to a recorded message	yes
editing capabilities for personal distribution lists	yes

Chapter 3

Logging on

In this chapter

Overview	3-2
Types of consoles	3-3
Logon/Status screen	3-4
Setting the system administration password	3-6
Changing the system administration password	3-8
Recovering a system administration password	3-10
Logging on from the main administration terminal	3-11
Logging on from a remote terminal	3-14
Changing the system time	3-17
Using a single terminal to access the switch and Meridian Mail Compact Option	3-18

Overview

Introduction

This chapter explains how to set your administration password and log on to the Meridian Mail Compact Option system from the following types of consoles:

- the main administration terminal
- a remote terminal

After you are logged on, you can begin to work with the system administration menus, which are the starting point for general administrative functions and for customizing your system.

The chapter also describes how to change or recover your administration password.

Types of consoles

Introduction

Administrative functions can be carried out from the main administrative console for your Meridian Mail Compact Option system or from a remote terminal connected to the system through a modem.

Console types

The following table lists the types of consoles and their available features.

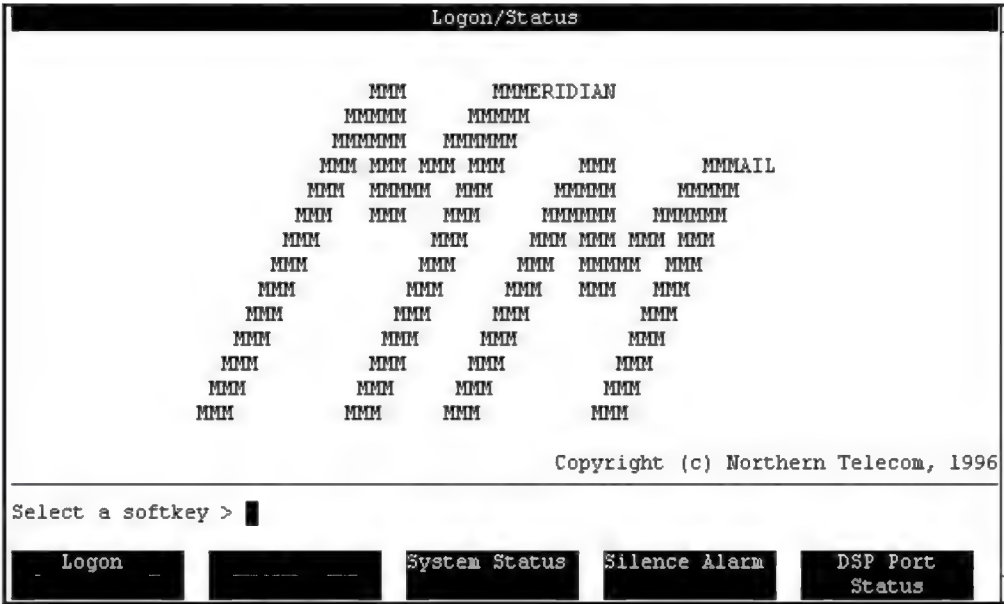
Main administration terminal	Remote terminal
installed with your system	available feature
all functions	generally used by off-site service personnel to troubleshoot a system

Logon/Status screen

- Description**
- From this screen, you log on to the administration console to perform the following tasks:
- setting up and customizing your system
 - carrying out administrative tasks on a system-wide basis, or a per-user basis
 - configuring voice services
 - viewing system status or DSP port status
 - silencing alarms

The Logon/Status screen is displayed when the administration terminal is idle.

The Logon/Status screen The following shows an example of the Logon/Status screen.



ATTENTION

For security and memory usage reasons, do not leave the administration console unattended while you are logged on. Also, remember to log out at night. If you do not log out, critical audit and backup routines may not run because of insufficient memory.

Available softkeys

For information about the softkeys available from the Logon/Status screen, [see Chapter 27, "System status and maintenance"](#).

Redrawing the Logon/Status screen

If you power down your terminal and then power it back up, the screen may be drawn incorrectly. If the screen is corrupted, you see a row of "q"s (qqqqqqqqqqqq) instead of the line near the bottom of the screen above the softkeys.

To redraw a corrupted screen, follow these steps.

Step	Action
1	Press <Ctrl> <w>.
	Result: A small window opens.
2	Type if .
	Note: You do not have to press <Return>. The "i" means initialize, and the "f" means full screen.

Setting the system administration password

Overview

To log on to the Meridian Mail Compact Option system from an administration terminal, you require a system administration password.

Your password can be any combination of letters and numerals. It can be between 1 and 16 characters long.

Passwords are not case sensitive; even if you use capital letters when you define your password, you do not need to use capital letters when you type it.

Password security

For greater system security, your password should be no fewer than seven characters in length. A longer password is more difficult to guess than a shorter password.

For more information about ensuring the security of your system, [see Chapter 6, "Setting up Meridian Mail Compact Option security"](#).

Procedure

To set your system administration password for the first time, follow these steps.

Starting Point: The Logon/Status screen

Step Action

- 1 Select the [Logon] softkey.
Result: The system prompts you for a password.
 - 2 Type the default password **adminpwd**.
Result: The system prompts you for a new password. It does not allow you to log on until you change the default password.
 - 3 Type a new password, and press <Return>.
Result: The system prompts you to reenter the password for verification.
 - 4 Type your new password a second time, and press <Return>.
Result: The system records the new password and displays the Main Menu.
Note: If you type a different password the second time, the system reports that the password has not changed because the new passwords did not match. If you receive this message, repeat [step 1](#) to [step 4](#).
-

Changing the system administration password

Introduction

When the Meridian Mail Compact Option system is first installed, you are given a default system administrator password (adminpwd). When you log on for the first time using this default password, you are prompted for a new password.

Password requirements

Passwords are not case sensitive; any capitalization used in defining the password need not be used when entering the password. The password can contain both alpha and numeric characters.

The minimum password length is 1 character, and the maximum length is 16 characters. It is recommended that your administration password be at least seven characters for added security. The longer the password, the better.

Frequency of password changes

Once you have initially changed your password, you should continue to change it on a regular basis.

For more information about ensuring the security of your system, [see Chapter 6, "Setting up Meridian Mail Compact Option security"](#).

Procedure

To change your system administration password, follow these steps.

Starting Point: The Main Menu

Step Action

- 1 Select General Administration.
 - 2 Select Change System Administrator Password.
Result: The system prompts you to enter your existing administration password.
 - 3 Type your existing password.
Note: Your password is not displayed on the screen as you type it.
Result: The system prompts you to enter a new password.
 - 4 Type your new password, and press <Return>.
Result: The system prompts you to reenter the password for verification.
 - 5 Type your new password a second time, and press <Return>.
Result: The system records the new password, and you are returned to the General Administration menu.
Note: If you type a different password the second time, the system reports that the password has not changed because the new passwords did not match. If you receive this message, repeat steps 2 to 5.
-

Recovering a system administration password

Introduction

This topic describes how to restore a password that has been forgotten or lost to the system.

Procedure

To recover a system administration password, follow these steps.

Starting Point: The Main Menu

Step	Action
------	--------

- | | |
|---|---|
| 1 | Insert the install tape in the tape drive. |
| 2 | Reboot the system from the tape. |
| 3 | Select More Utilities from the menu. |
| 4 | Select Change to Default System Password.
Result: You are prompted to enter Yes to continue, or No to stop. |
| 5 | Enter Yes to continue.
Result: The system reports that the operation has been successfully completed. |
| 6 | Remove the install tape from the tape drive. |
| 7 | Reboot the system from the disk. |
| 8 | Select the [Logon] softkey.
Result: The system prompts you for a password. |

Step Action

- 9 Type the default password **adminpwd**.
Result: The system prompts you for a new password. It does not allow you to log on until you change the default password.
- 10 Type a new password, and press <Return>.
Result: The system prompts you to reenter the password for verification.
- 11 Type your new password a second time, and press <Return>.
Note: If you type a different password the second time, the system reports that the password has not changed because the new passwords did not match. If you receive this message, repeat [step 8](#) to [step 11](#).
-

Logging on from the main administration terminal

Introduction

This topic explains how to log on as the system administrator from the main administration terminal.

Note: If you are logging on from a multiple administration terminal, you cannot perform [step 2](#).

Procedure

To log on from the main administration terminal, follow these steps.

Starting Point: The Logon/Status screen

Step	Action
------	--------

1	Select the [Logon] softkey.
---	-----------------------------

Result: The system prompts you for a password.

2	Use the following table to determine the next step.
---	---

IF	THEN
you are logging on for the first time	see "Setting the system administration password" on page 3-6.
you have logged on before	go to step 3.

3	Type your system administration password, and press <Return>.
---	---

Result: The system displays the Main Menu.

Note: If an invalid password is entered, an error message appears. Repeat [step 1](#) and [step 3](#).

The Main Menu

The following shows an example of the Main Menu displayed at the main administration terminal.

The screenshot shows a terminal window titled "Main Menu". Inside, there is a numbered list of nine options: 1 User Administration, 2 General Administration, 3 Voice Administration, 4 Hardware Administration, 5 System Status and Maintenance, 6 Operational Measurements, 7 Network Administration, 8 Class of Service Administration, and 9 Bulk Provisioning. Below the list is a prompt "Select an item >" followed by a cursor. At the bottom of the window, there is a "Logoff" button and four other unlabeled buttons.

```
Main Menu

1 User Administration
2 General Administration
3 Voice Administration
4 Hardware Administration
5 System Status and Maintenance
6 Operational Measurements
7 Network Administration
8 Class of Service Administration
9 Bulk Provisioning

Select an item > █

Logoff [ ] [ ] [ ] [ ]
```

Note: Some of these features may not be available on your system.

ATTENTION

An unsuccessful logon attempt is automatically recorded in the system log file. As a security precaution, after a third unsuccessful attempt to log on, the system forces a 10-minute delay before a further logon attempt is accepted. Only your Northern Telecom (Nortel) representative has the required privileges to gain access to the system during the lockout period.

Logging on from a remote terminal

Introduction

This topic explains how to log on to the system through a remote terminal.

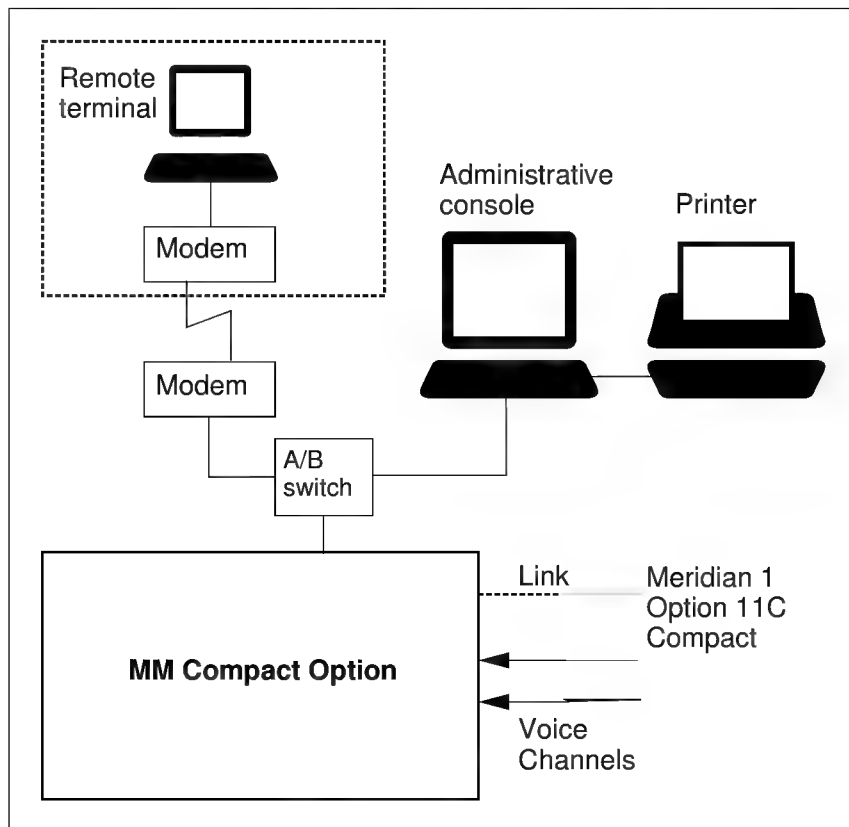
If your installation has a remote administration terminal installed for service personnel, administrative functions can be performed remotely.

Your logon password is the same for both the main administration terminal and the remote terminal.

The administrative functions described in this guide are identical whether viewed from the local administration terminal or from the remote terminal.

Typical remote terminal configuration

The following diagram shows a typical remote terminal configuration for an Meridian Mail Compact Option system.



g100106a

Coordinating a remote logon

Because no administrative functions can be carried out from the local console while a remote logon is in effect, a remote logon should be coordinated with the local administrator.

Logging on from a remote terminal

To log on from a remote terminal, follow these steps.

Starting Point: The Logon/Status screen at the local administration console

Step	Action
1	Change the A/B switch setting to remote.
2	Notify the user at the remote terminal. The user at the remote terminal does the following: a. Dial in to the modem. b. Press <Ctrl> <r> to display the Logon screen. c. Type the administration password. d. Carry out administrative tasks as required, and then log off.

Disabling remote terminal access

To disable remote terminal access, follow these steps.

Step	Action
1	At the local site, change the A/B switch back to the local setting. Result: Control is returned to the local console where the Logon/Status screen is again displayed.

Changing the system time

Introduction

The Meridian Mail Compact Option system gets its time from the Option11C Compact. It receives time stamps passed from the switch at regular intervals. However, you can set up your Meridian Mail Compact Option database while the link to the switch is down. If you will be configuring the database when the link is not operational, you will have to set the system time on the Meridian Mail Compact Option side. Then, once the link is up, the switch time will override the Meridian Mail Compact Option time.

Procedure

To change the system time, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. Result: The General Administration screen appears.
2	Select Change System Time. Result: You are prompted to enter the date and time.
3	Enter the date and time, and press <Return>. Result: The clock is synchronized to the clocking signals from the network, the time is recorded, and the General Administration screen is redisplayed.
4	When you have set the system time, press <Exit>.

Using a single terminal to access the switch and Meridian Mail Compact Option

Introduction

If you are logging on at a site with only one terminal access, then you will need to move back and forth between the Option11C Compact and Meridian Mail Compact Option.

Procedure

Follow these steps to toggle between the switch and Meridian Mail Compact Option. You use the same terminal to access both Meridian Mail Compact Option and the Option11C Compact.

Step Action

- 1 Press <Control>] to switch to the Option11C Compact display from Meridian Mail Compact Option.
- 2 Enter **AX** <Return> to return to the Meridian Mail Compact Option display.

Note: You are returned to the system administrator screen you were using when you accessed the switch.

Note: On Software release 22 if there is more than one link configured, enter AX n<Return>, where n is the TTY number of the link to which you are connecting. In most Meridian Mail Compact Option installations this will be 8, therefore enter AX 8<Return>.

If you have any problems accessing the Option11C Compact, refer to the appropriate chapters of *Option 11C Compact Planning, Installation and Fault Clearing Guide* (NTP 553-3121-210.)

Chapter 4

Setting up the system

In this chapter

Overview	4-2
Changing the system administration password	4-3
Checking the hardware configuration	4-4
Checking the system status	4-5
Checking the Channel Allocation Table	4-6
Configuring general system options	4-7
Setting up dialing translations	4-8
Setting up restriction and permission lists	4-9
Customizing voice messaging options	4-10
Adding DNs to the VSDN table	4-11
Defining classes of service	4-12
Configuring operational measurement options	4-13
Adding users to the system	4-14
Creating system distribution lists	4-15
Setting up the Voice Menus feature	4-16
Setting up the Enterprise Networking feature	4-17
Setting up system security	4-18
Backing up the system	4-19

Overview

Introduction

This chapter provides general information and procedures for checking the provisioning of your Meridian Mail Compact Option system. Wherever necessary, it refers you to more detailed information in other chapters of this guide and in other manuals.

It also provides an overview of a complete basic setup of your system.

Objective

This section is intended as a checklist for system setup.

Before you begin

To ensure that your Meridian Mail Compact Option system is properly provisioned, refer to the procedures in the *Option 11C Compact Planning, Installation and Fault Clearing Guide* (NTP 553-3121-210).

Changing the system administration password

Introduction

This involves logging on to the main administration terminal using the current password, and then following the system instructions to change the password.

Procedure

For information and procedures for changing the system administration password, [see Chapter 3, "Logging on"](#).

Checking the hardware configuration

Introduction

This involves checking the node configuration and the data port configuration.

Check the data port configuration to verify the assignment of data devices, especially parameters such as the baud rate and parity for the administration console.

Procedure

To check the hardware configuration, refer to the procedures in the *Option 11C Compact Planning, Installation and Fault Clearing Guide* (NTP 553-3121-210).

Checking the system status

Introduction

This involves verifying the status of the system and enabling or disabling system nodes and DSP ports.

Procedure

For information and procedures for checking the system status, see Chapter 27, "System status and maintenance".

Checking the Channel Allocation Table

Introduction

This involves configuring the primary DN and Channel DN for each agent/channel. It also involves configuring the service or services for which the channel will be used. In most cases, channels are shared by all services. If any channels are to be dedicated to a specific service, enter the service in the Channel Allocation Table.

You check the Channel Allocation Table to ensure consistency between the switch and the Meridian Mail Compact Option system.

Note: This step should be carried out only by a qualified technician.

Procedure

To check the Channel Allocation Table, see “Channel Allocation Table” on page 27-45.

Configuring general system options

Introduction

This involves viewing the features that are installed on your system and configuring the attendant DN and date format for reports. The General Options screen is also where you assign classes of service to the system. You can also modify the SEER and Reports printer port names if different from the console port.

Procedure

For information and procedures for configuring general system options, see Chapter 13, "General options".

Setting up dialing translations

Introduction

This involves defining network access prefixes for local off-switch, long distance, and international dialing, and for dialing translation tables.

Procedure

For information and procedures for setting up dialing translations, see Chapter 16, "Dialing translations".

Setting up restriction and permission lists

Introduction

This involves modifying the restriction and permission codes to allow users to dial only the external phone numbers or internal extension numbers that you specify. Unless you are upgrading from an earlier release of Meridian Mail Compact Option, features such as Mailbox Thru-Dial, Custom Revert DN, or Extension Dialing are initially restricted and do not work until you modify the restriction and permission codes.

You define restriction and permission codes to prevent external callers or internal users from placing local or long distance calls that you do not want billed to your system.

Note: This is a very important step.

Procedure

For information and procedures for setting up restriction and permission lists, [see Chapter 6, "Setting up Meridian Mail Compact Option security"](#).

Customizing voice messaging options

Introduction

This involves setting voice messaging parameters which includes such tasks as setting the broadcast mailbox number, the maximum allowed delayed for timed delivery, and the name dialing prefix.

Procedure

For information and procedures for customizing voice messaging options, see Chapter 19, "Voice messaging options".

Adding DN's to the VSDN table

Introduction

The VSDN table lists the DN's associated with specific voice services. A DN is required for each voice service that you want users to be able to access directly by dialing a unique DN. The VSDN table maps voice services onto DN's so that when your Meridian Mail Compact Option system receives an incoming call, it looks up the DN to determine which service is being requested and which prompts to play.

You define a DN in the VSDN table for each voice service that is to be directly dialable by internal users or external callers. This includes services such as voice messaging and express messaging.

Before you begin

For each service you plan to add to the VSDN table, an existing ACD queue must already be configured on the Option11C Compact.

Procedure

For information and procedures for adding DN's to the VSDN table, see Chapter 23, "The VSDN table".

Defining classes of service

Introduction

This involves identifying which of your users have similar needs and what those needs are, and then defining the operating parameters or Class of Service (COS) for each group of users.

When you change a parameter in a COS, all users belonging to that COS have the changes automatically updated.

ATTENTION

You must add classes of service before you add users.
Each user must be assigned to a class of service.

Procedure

For information and procedures for defining classes of service, see Chapter 25, "Class of Service administration".

Assigning COSs to the system

After you add classes of service you must assign them to the system. If you do not do this, the classes of service will not show up in the Add a Local Voice User screen and you will not be able to assign them to users.

Classes of service are assigned to the system in the General Options screen.

Configuring operational measurement options

Introduction

This involves defining how system and user statistics are collected. This includes, for example, the kinds of data to be collected, the time that traffic data collection begins and ends each day, and how often collected traffic statistics are written to disk.

You do not need to configure the operational measurement options right away. You may choose instead to use the default settings.

You can then modify these settings after your system has been in use for a time to provide a level of detail that is more appropriate for your needs.

Procedure

For information and procedures for configuring operational measurement options, see Chapter 29, "Operational Measurements".

Adding users to the system

Introduction

This involves a number of tasks. Before you begin, you need to determine the capacity of your disk volume, survey users to establish the classes of services that will be necessary, estimate the average system usage of each class of user, and create classes of service to reflect your research.

You also identify users as local voice users, remote voice users, or directory entry users according to their needs.

Procedure

For information and procedures for adding users to the system, see the following chapters.

For information about	See
user administration in general	Chapter 7 , “User administration—an overview”
local voice users	Chapter 8 , “Local voice users”
remote voice users	Chapter 9 , “Remote voice users”
directory entry users	Chapter 10 , “Directory entry users”
distribution lists	Chapter 11 , “Distribution lists”

Creating system distribution lists

Introduction

A distribution list is a collection of mailbox numbers. It allows you to send the same message to a number of people. Distribution lists are convenient if you frequently have to send messages to the same group or groups of people.

You do not need to create system distribution lists as part of the initial configuration. If you know which lists you need, then you can create them, but they can be created at any time.

Procedure

For information and procedures for creating system distribution lists, see Chapter 11, "Distribution lists".

Setting up the Voice Menus feature

Introduction

The Voice Menus feature enables you to create a number of custom call answering applications.

The Announcements service allows you to record messages that can be played back within a voice menu or as a stand-alone service that can be dialed directly.

Thru-Dial services access predefined DNs or user-prompted DNs that can be used either within a voice menu service or as a separate service with a directory number. Thru-Dial services can be set up to allow Name Dialing and can have restrictions barring users from dialing unauthorized numbers, such as long distance access codes.

The Time-of-Day Controllers service allows you to control the activation of voice services based on the date and time at which a call is received. This allows you to control the availability of voice services during off-hours and holidays.

The Voice Menus service enables you to create single-layered or multilayered menus that present callers with a series of choices about the action they can perform.

The Voice Prompt Maintenance service enables you to modify the prompts and greetings available in your voice menus and announcements using a telephone.

The Remote Activation service allows you to enable or disable voice services while you are offsite through a standard dual-tone multifrequency (touch tone) telephone set.

Setting up the Enterprise Networking feature

Introduction

Enterprise Networking is a Meridian Mail Networking protocol that permits one or more Meridian Mail Compact Option systems to send messages to and receive messages from users at remote Meridian Mail Compact Option sites. It uses the following:

- a network database to define local and remote sites
- DTMF signaling based on the AMIS protocol, instead of modems, to transmit messages between sites

Procedure

For information and procedures for setting up the Enterprise Networking feature, refer to *Meridian Mail Compact Option Enterprise Networking Installation and Administration Guide* (NTP 555-7001-222).

Setting up system security

Introduction

In today's telecommunications environment, every computerized system is potentially open to unauthorized access. It is necessary to take all possible precautions to prevent security breaches.

If your system is properly secured, it is difficult for a user connected to Meridian Mail Compact Option (such as a user who is logged on to a mailbox or an external caller who has connected to Meridian Mail Compact Option through a call answering session or a voice menu) to place unauthorized calls that will be billed to your system.

Procedure

For information and procedures for setting up system security, [see Chapter 6, "Setting up Meridian Mail Compact Option security"](#).

Backing up the system

Introduction

After you have finished customizing your system configuration, back up the new data onto tape to ensure its safety. This involves making backup copies of some or all of the system's data.

In the event of disk failure, you will not need to reenter user and site-specific information, and you can bring your system back into service quickly.

Procedure

For information and procedures for backing up the system, see Chapter 15, "Back up and restore Meridian Mail Compact Option data".

Chapter 5

Making voice recordings

In this chapter

Overview	5-2
Types of recordings	5-4
Voice recording tips	5-7
Logging in to Meridian Mail Compact Option	5-9
Recording a call answering greeting	5-13
Recording personal greetings	5-19
Recording a personal verification	5-21
Recording a personal verification for a system distribution list	5-26
Identifying remote site names	5-29
Recording a personal verification for the broadcast mailbox	5-33
Recording and sending broadcast messages	5-36
Making Voice Services recordings	5-38

Overview

Introduction

As an administrator, you make two types of voice recordings: those used only for administrative purposes, and those played to the public or other users. You make these recordings through the administration terminal (with a telephone nearby) or by using a telephone handset alone.

This chapter provides information and procedures for making different kinds of voice recordings or, where necessary, refers you to other chapters or manuals for this information.

The overview presents an introduction to the types of voice recordings you can make. It also offers some guidelines for making voice recordings.

Introduction

This chapter presents information and procedures for logging in to Meridian Mail Compact Option and creating, playing back, editing, and deleting recordings.

These recordings include the following:

- the call answering greeting
- personal verifications (which can be recorded by you or the users on your system)
- system distribution list personal verifications
- remote site name verifications
- broadcast mailbox personal verifications
- Voice Services recordings (announcements, Thru-Dial services, voice menus, and Voice Prompt Maintenance)

For your reference, this chapter also presents an overview of some of the voice recordings that users on your system make. These include the following:

- personal greetings
- broadcast messages

Types of recordings

Introduction	You can make different kinds of voice recordings from the administration terminal and a telephone or from a telephone handset alone. This overview presents an introduction to these recordings.
Call answering greeting	The call answering greeting in Meridian Mail Compact Option identifies your organization to external callers. You record the call answering greeting from the administration terminal or from a telephone handset with administrator capabilities. For information and procedures, see “Recording a call answering greeting” on page 5-13.
Personal greetings	Meridian Mail Compact Option users can record three kinds of personal greetings from their telephone handsets: external, internal, and temporary absence greetings. For information and procedures, see “Recording personal greetings” on page 5-19.
Personal verification	The personal verification is used to identify local, remote, or directory entry users. Typically, it is recorded by the users themselves from their telephones, but you can also record it from the administration terminal as you add a user to the system or if you are logged into a mailbox as administrator. For information and procedures, see “Recording a personal verification” on page 5-21.

System distribution list personal verification

The system distribution list personal verification is an optional recording. This verification helps you to confirm you have selected the correct distribution list when you enter its number as you compose a message. The list title can describe who is included in the list or the purpose of the list.

For information and procedures, [see “Recording a personal verification for a system distribution list” on page 5-26.](#)

Remote site name verification

The remote site name verification works like a personal verification for network sites. You record the site name verification from the administration terminal. It is used to confirm the site name when a message is addressed or when users receive a message from a network site.

For information and procedures, [see “Identifying remote site names” on page 5-29](#), and refer to the *Meridian Mail Compact Option Enterprise Networking Installation and Administration Guide* (NTP 555-7001-222).

Broadcast mailbox personal verification

A broadcast message is a message that is sent to all Meridian Mail Compact Option users.

You can record a personal verification for the broadcast mailbox so that when you enter the mailbox number during message composition, you get a verification that you have entered the correct number.

The personal verification for a broadcast mailbox can say something like: *“Broadcast mailbox 5555.”*

For information and procedures, [see “Recording a personal verification for the broadcast mailbox” on page 5-33](#)”.

Broadcast messages A broadcast message is a message that is sent to all Meridian Mail Compact Option users.

When you or the users on your system compose a message to the broadcast mailbox, the message is sent to all of the users on the system.

For more information and procedures, [see “Recording and sending broadcast messages” on page 5-36.](#)

Voice Services recordings The Voice Services feature enables you to create custom call answering applications. Voice services recordings include announcement recordings, Thru-Dial greetings, voice menu greetings, voice menu choices, and voice menu prompts.

For more information and procedures, [“Making Voice Services recordings” on page 5-38.](#)

Voice recording tips

Introduction

As administrator, you make two types of voice recordings:

- prompts that are used only for administrative purposes (such as broadcast mailbox personal verifications or system distribution list personal verifications)
- recordings played to the public or other users (such as the call answering greeting, personal verifications, remote site name verifications, and Voice Services recordings such as announcements, Thru-Dial services, or voice menus)

Prompts used only for administrative purposes require little preparation after you decide on their wording.

Voice menus or announcements played to the public or other users may require more formal preparation.

Guidelines for voice recordings

The following are some suggestions for making voice recordings:

- Use only one voice for your voice recordings, so that callers are not distracted by changes in pitch, tone, intonation, or accent.
- To select a person to make your voice recordings, begin by auditioning a few candidates. Record their voices and then listen to the recordings over the telephone line. Low-pitched voices reproduce better than high-pitched voices over telephone lines. The voice used for the Meridian Mail Compact Option prompts provides a good model.
- Print out complete, definitive copies of the script.
- Record in quiet surroundings.

Start recording immediately after the tone, and stop the recording immediately after the last word. This prevents unnecessary pauses when system prompts and personal verifications are joined.

- To stop recording, press the number sign (#) if you are recording from a telephone handset or the [Stop] softkey if

you are recording from the administration terminal. Do not hang up the phone while you are recording as this may produce clicks in the recording.

- For applications that provide current information, have the person who knows the information monitor the prompts to ensure that the information is always up-to-date.

Logging in to Meridian Mail Compact Option

Introduction

Before you can create, play back, modify, or delete voice recordings, you need to log in to Meridian Mail Compact Option. You do this either through a telephone set or through an administration terminal with a telephone nearby.

About using the telephone to make recordings

Using a telephone on your system, you or the users on your system log into Meridian Mail Compact Option and access personal greetings. You can then make a number of kinds of voice recordings:

- external, internal, and temporary absence greetings
- personal verifications
- broadcast messages

About using a terminal to make recordings

Using the administration terminal or a telephone set with administrator capabilities, you can make certain kinds of recordings:

- the call answering greeting
- personal verifications
- system distribution list personal verifications
- site name verifications
- broadcast mailbox personal verifications
- Voice Services recordings

To make recordings through the system interface, the [Voice] softkey must be displayed.

Note: A telephone set is required to make recordings through the administration terminal. Ensure that a phone set is available near the administration terminal where you are working.

Screens with recording softkeys

Recording softkeys are available from some of the User Administration screens and Voice Services Administration screens.

Recording softkey positions

The following shows typical recording softkey positions.



Logging in using a telephone

To log in to Meridian Mail Compact Option using a telephone set, follow these steps.

Step Action

- 1 Dial the Meridian Mail Compact Option access number.
- 2 Use the following table to determine the next step.

IF you are logging in from THEN	
your own telephone	press #.
another touch tone telephone	using the telephone keypad, enter your mailbox number, and press #.

Step Action

- 3 Enter your password using the telephone keypad, and press #.
- 4 Use the following table to determine the next step.

IF you want to	THEN
create, play back, modify, or delete an internal greeting	see "Recording personal greetings" on page 5-19.
create, play back, modify, or delete an external greeting	see "Recording personal greetings" on page 5-19.
create, play back, modify, or delete a temporary absence greeting	see "Recording personal greetings" on page 5-19.
create, play back, or delete a personal verification	see "Recording a personal verification" on page 5-21.

Logging in from the administration terminal

To log in to Meridian Mail Compact Option from the administration terminal, follow these steps.

Starting Point: The Logon/Status screen

Step Action

- 1 Select [Logon].

Result: *The system prompts you for a password.*

- 2 Use the following table to determine the next step.

IF	THEN
you are logging in the first time	see "Setting the system administration password" on page 3-6.
you have logged in before	go to step 3.

- 3 Type your system administration password, and press <Return>.

Result: *The system displays the Main Menu.***Note:** If an invalid password is entered, an error message appears. Return to [step 1.](#)

- 4 Use the following table to determine the next step.

IF you want to record	THEN
the call answering greeting	see "Recording a call answering greeting" on page 5-13.
a personal verification	see "Recording a personal verification through the administration terminal" on page 5-24.
a personal verification for a system distribution list	see "Recording a personal verification for a system distribution list" on page 5-26.
a personal verification for a remote site name	see "Identifying remote site names" on page 5-29.
a broadcast mailbox personal verification	see "Recording a personal verification for the broadcast mailbox" on page 5-33.
make Voice Services recordings	see "Making Voice Services recordings" on page 5-33.

Recording a call answering greeting

Introduction

This topic provides information and procedures for recording a call answering greeting.

The call answering greeting identifies your organization to callers and users. Typically, this greeting consists of the spoken name of the organization.

The call answering greeting is played when

- an external caller is transferred to Meridian Mail Compact Option to leave a message

You record the call answering greeting from the administration terminal or from a telephone set with administrator capability.

Using the call answering greeting

This greeting is optional. If you record the greeting, external callers hear it before they hear a user's personal greeting. If no greeting is recorded, callers hear only the user's personal greeting when they connect to a mailbox.

When a call answering greeting exists, the following prompt is played: *"Hello. <Call Answering Greeting> has received a message for"*

Guidelines for composing

The following are some guidelines for composing a call answering greeting:

- Because this greeting is used in a variety of situations, consider how best to word it (or decide whether you want to record a greeting at all).
- If you do not record a call answering greeting, your organization's name is not announced at the beginning of a call answering session. If you feel that the user's personal greeting is sufficient, you may regard the call answering greeting as unnecessary.
- If you record only the organization's name ("*Myelin Incorporated*"), the greeting played during call answering may be too abrupt. A friendlier greeting ("*Thank you for calling Myelin Incorporated*") is ideal for call answering.

Multilingual systems

If more than one language is installed on your Meridian Mail Compact Option system and you want to record a call answering greeting, you need to record one greeting for each language.

Recording the call answering greeting from a telephone set

To record, play back, modify, or delete the call answering greeting from a telephone set with administrator capabilities, follow these steps.

Step Action

- 1 Press **82** on the telephone keypad.
- 2 Press **9** for the system greeting.
- 3 Use the following table to determine the next step.

IF you want to	THEN
review the greeting	go to step 4 .
delete the greeting	go to step 5 .
rerecord the greeting	go to step 5 .
add to the greeting	go to step 6 .
- 4 To review the greeting, press **2**.
- 5 To delete the greeting, press **76**.
Note: If you do not delete the existing greeting, your new recording is appended to it.
- 6 To begin recording or add to the greeting, press **5**.
- 7 At the tone, record the call answering greeting.
- 8 To stop recording, press **#**.
Note: Do not hang up the phone during recording as this may produce a click sound.
- 9 To review the greeting, press **2**.
- 10 To end your voice messaging session, press **83**, and then hang up.

Procedure

To create, play back, modify, or delete a call answering greeting through the administration terminal, follow these steps.

Starting Point: The Main Menu

Step Action

1 Select Voice Administration.

2 Select Voice Messaging Options.

Result: The system displays the Voice Messaging Options screen.

Voice Administration	
Voice Messaging Options	
Default Language:	American_English Canadian_French
Default Language Overrides User's Preferred Language for Call Answering:	No Yes
Customized recording for American_English	
Call Answering Greeting (Voice):	No
Customized recording for Canadian_French	
Call Answering Greeting (Voice):	No
Maximum Delay for Timed Delivery (days):	31
MORE BELOW	
Save	Cancel
	Voice

3 Move the cursor to the first Call Answering Greeting (Voice) field.

4 Select the [Voice] softkey.

Result: The current screen remains displayed; the softkey display changes to [Cancel].

The system prompts for an extension number.

5 Type the extension number of the telephone set you will use to make the recording, and press <Return>.

Result: The phone rings.

Step Action

- 6 Pick up the telephone handset.
Result: The system displays the recording softkeys.
- 7 Select the [Record] softkey.
Result: The system displays the [Stop] softkey in place of the [Record] softkey.
You hear a tone through the telephone receiver.
- 8 At the tone, begin speaking into the receiver.
Note: Recording stops automatically if the greeting exceeds the Maximum Prompt Size or the Record Timeout set in the Voice Services Profile.
- 9 To stop recording, select the [Stop] softkey.
Result: The recording stops automatically, and the system again displays the recording softkeys.
- 10 Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11.
delete the recording	go to step 13.
record the greeting again	go to step 7.
save the recording	go to step 17.

- 11 Select the [Play] softkey.
Result: If a recording is available, it is played.
The system displays the [Stop] softkey.
Note: If there is no current recording, the system displays a message on the console.
- 12 To stop the playback at any time, select the [Stop] softkey.
Result: The system again displays the recording softkeys.
- 13 To delete the recording, select the [Delete] softkey.
Result: The system displays the [OK to Delete] and [Cancel] softkeys.
You are requested to confirm the deletion.

Step Action

-
- | | |
|----|---|
| 14 | Use the following table to determine the next step. |
|----|---|
- | | |
|-----------------------|--------------------------------|
| IF you want to | THEN |
| cancel the deletion | go to step 15. |
| confirm the deletion | go to step 16. |
-
- | | |
|----|---|
| 15 | <p>To cancel the deletion, select the [Cancel] softkey.</p> <p>Result: The recording is not deleted.</p> <p>The system again displays the recording softkeys.</p> |
| 16 | <p>To delete the recording, select the [OK to Delete] softkey.</p> <p>Result: The system deletes the recording.</p> <p>The system again displays the recording softkeys.</p> |
| 17 | <p>To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone.</p> <p>Result: The system displays the original softkeys.</p> <p>Note: When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey.</p> <p>When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.</p> |
| 18 | <p>To update the screen and store the changes to the recording, use the [Save] softkey.</p> |
-

Recording personal greetings

Introduction

You and the users on your system record personal greetings—external, internal, and temporary greetings—from the telephone. These recordings are played when callers connect to a mailbox.

Recording personal greetings

To create, play back, modify, or delete a personal greeting, follow these steps.

Note: You must be logged in to a mailbox. [See “Logging in to Meridian Mail Compact Option” on page 5-9.](#)

Step Action

- 1 Press **82** on the telephone keypad.
- 2 Select an external, internal, or temporary absence greeting.

IF you want to select	THEN
your external greeting	press 1 .
your internal greeting	press 2 .
your temporary absence greeting	press 3 .

Result: The system confirms the greeting you select.

- 3 Use the following table to determine the next step.

IF you want to	THEN
review your greeting	go to step 4 .
delete your greeting	go to step 5 .
record your greeting again	go to step 5 .
add to your greeting	go to step 6 .
set an expiry date for your temporary absence greeting	go to step 9 .

- 4 To review the greeting, press **2**.

Step	Action
------	--------

- | | |
|----|---|
| 5 | To delete the greeting, press 76 .
Note: If you do not delete your existing greeting, your new recording is appended to it. |
| 6 | To begin recording or add to the greeting, press 5 . |
| 7 | At the tone, record your greeting. |
| 8 | To stop recording, press # .
Note: Do not hang up the phone during recording as this may produce a click sound. |
| 9 | To set the expiry date for your temporary absence greeting, press 9 .
Note: Whenever you log in to your mailbox, the system prompts that you are using a temporary greeting if the expiry date is not set. |
| 10 | To end your voice messaging session, press 83 , and then hang up. |
-

Recording a personal verification

Introduction

This topic provides information and procedures for recording a personal verification using either a telephone handset alone or the administration terminal and a telephone.

The personal verification is a recording of a user's first and last names (and extension, if desired). It is used to identify the owner of a mailbox. Ideally, users should record personal verifications in their own voice. However, as administrator, you can record personal verifications for users either from the administration terminal or from a telephone set with administrator capabilities.

Using a personal verification

A personal verification is played in the following situations:

- In Call Answering, the personal verification is played if no personal greeting has been recorded.
- During message composition, the system plays the verification after a user enters a mailbox number to verify that the correct person is being addressed.
- When a user receives a message, the system plays the verification to identify who the message is from (such as the system administrator) or to advise all recipients that the message is a broadcast message.
- When callers use the Name Dialing feature, the system plays the personal verification. If a personal verification has not been recorded, the system spells out the name instead.
- During Express Messaging, the system plays the personal verification.

If no verification is recorded, the system plays a recording of the user's extension number. Because it is easier for callers to confirm they have reached the correct person by hearing a name rather than by hearing an extension number, it is highly recommended that you or the users on your system record a personal verification for each mailbox.

Using a personal verification (continued)

Users can change their personal verifications only if this capability is enabled in the class of service to which they are assigned. For more information, see Chapter 25, "Class of Service administration".

Guidelines for composing

The following are some suggestions for recording personal verifications:

- Record a few names for personal verification, and listen to them before recording the remaining names.
This ensures that the procedure is done correctly and the intonation is good. Test each of the following areas where personal verification applies:
 - call answering greeting
 - message envelope playback
 - address playback in the compose command
 - name dialing
 - name addressing
- When you are recording a personal verification for two or more people in your organization who have the same name (or very similar names), provide more information (their extension number or title, for example) to distinguish them.

Recording a personal verification using a telephone

To create, play back, or delete a personal verification using a telephone handset, follow these steps.

Note: You must be logged in to a Meridian Mail Compact Option mailbox. [See “Logging in to Meridian Mail Compact Option” on page 5-9.](#)

Step Action

- 1 Press **89** on the telephone keypad.
Result: The system plays the existing name for personal verification.
 If no name is recorded, the system reports this.
- 2 Use the following table to determine the next step.

IF you want to	THEN
hear the name for personal verification again	go to step 3 .
record a new personal verification	go to step 4 .
delete the existing personal verification	go to step 8 .
- 3 To hear the name for personal verification again, press **2**.
- 4 To record a new personal verification, press **5**.
- 5 At the tone, record your greeting.
Note: The maximum length is 20 seconds.
- 6 To stop recording, press **#**.
Result: The system replays your recording.
- 7 To add to the recording, press **5**, and repeat [step 5](#) and [step 6](#).
- 8 To delete the existing personal verification, press **76**.
- 9 To end your voice messaging session, press **83**, and then hang up.

Recording a personal verification through the administration terminal

To create, play back, or delete a personal verification from the administration terminal, follow these steps.

Starting Point: The Main Menu

Step Action

- 1 Select User Administration.
- 2 Select Local Voice User.
- 3 Select the [View/Modify] softkey, and type the mailbox number of the user whose personal verification you want to record.
Result: The system displays the View/Modify Local Voice User screen.
- 4 Select the [Voice] softkey.
Result: The current screen remains displayed; the softkey display changes to [Cancel].
The system prompts for an extension number.
- 5 Type the extension number of the telephone set you will use to make the recording, and press <Return>.
Result: The phone rings.
- 6 Pick up the telephone handset.
Result: The system displays the recording softkeys.
- 7 Select the [Record] softkey.
Result: The system displays the [Stop] softkey in place of the [Record] softkey.
You hear a tone through the telephone receiver.
- 8 At the tone, begin speaking into the receiver.
Note: Recording stops automatically if the recording exceeds the Maximum Prompt Size or the Record Timeout set in the Voice Services Profile.
- 9 To stop recording, select the [Stop] softkey.
Result: The recording stops automatically, and the system again displays the recording softkeys.

- 10 Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11.
delete the recording	go to step 14.
record the verification again	go to step 7.

- 11 To review your recording, select the [Play] softkey.
Result: The system plays the recording.
 The system displays the [Stop] softkey.
- 12 To stop the playback at any time, select the [Stop] softkey.
Result: The system again displays the recording softkeys.
- 13 To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone.
Result: The system displays the original softkeys.
Note: When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey.
 When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
- 14 To delete a personal verification, use the arrow keys to select the entry, select the name using the spacebar, and press [Delete].
Result: The system displays the [OK to Delete] and [Cancel] softkeys.
- 15 Select [OK to Delete] to delete the personal verification.
Result: The system deletes the personal verification and updates the list.
- 16 To update the screen and store the changes to the recording, use the [Save] softkey.

Recording a personal verification for a system distribution list

Introduction

It is a good idea to make a voice recording of the title of each system distribution list. This procedure is optional, but a voice title helps you to confirm you have selected the correct list when you enter its number as you compose a message. The list title can describe who is included in the list or the purpose of the list.

Procedure

To record a personal verification for a system distribution list, follow this procedure.

Note: This procedure is optional.

Starting Point: The Main Menu

Step	Action
------	--------

- | | |
|---|---|
| 1 | Select User Administration. |
| 2 | Select Distribution Lists.
Result: The system displays the Distribution Lists softkeys screen. |
| 3 | Select the [View/Modify] softkey.
Result: The system prompts for a distribution list number. |
| 4 | Type the number of the distribution list for which you are recording a title. |
| 5 | Select the [Voice] softkey.
Result: The system prompts for an extension number. |
| 6 | Type the extension number of the telephone set you are going to use to record the title, and press <Return>.
Result: The phone rings. |
| 7 | Pick up the telephone handset.
Result: The system displays the recording softkeys. |

Step Action

- 8 Select the [Record] softkey.
Result: The system displays the [Stop] softkey in place of the [Record] softkey.
 You hear a tone through the telephone receiver.
- 9 At the tone, begin speaking into the receiver.
Note: Recording stops automatically if the recording exceeds the Maximum Prompt Size or the Record Timeout set in the Voice Services Profile. At the tone, record the personal verification.
- 10 To stop recording, select the [Stop] softkey.
Result: The recording stops automatically, and the system again displays the recording softkeys.
- 11 Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11.
delete the recording	go to step 14.
record the verification again	go to step 8.

- 12 To review your recording, select the [Play] softkey.
Result: The system plays the recording.
 The system displays the [Stop] softkey.
- 13 To stop the playback at any time, select the [Stop] softkey.
Result: The system again displays the recording softkeys.
- 14 To delete the recording, select the [Delete] softkey.
Result: The system displays the [OK to Delete] and [Cancel] softkeys.
 You are requested to confirm the deletion.
- 15 Use the following table to determine the next step.

IF you want to	THEN
cancel the deletion	go to step 16.
confirm the deletion	go to step 17.

Step	Action
------	--------

- | | |
|----|---|
| 16 | <p>To cancel the deletion, select the [Cancel] softkey.</p> <p>Result: The recording is not deleted.</p> <p>The system again displays the recording softkeys.</p> |
| 17 | <p>To delete the recording, select the [OK to Delete] softkey.</p> <p>Result: The system deletes the recording.</p> <p>The system again displays the recording softkeys.</p> |
| 18 | <p>To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone.</p> <p>Result: The system displays the original softkeys.</p> <p>Note: When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey.</p> <p>When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.</p> |
| 19 | <p>To update the screen and store the changes to the recording, use the [Save] softkey.</p> |
-

Identifying remote site names

Introduction

The site name verification works like a personal verification for network sites. You record the site name verification from the administration terminal. It is used to confirm the site name when a message is addressed or when users receive a message from a network site. A site name can be recorded for Meridian Mail Compact Option network sites.

If no site name is recorded, the system instead plays a recording of the site or location number that identifies the site.

For more information refer to the *Meridian Mail Compact Option Enterprise Networking Installation and Administration Guide* (NTP 555-7001-222).

Remote site name verification

The site name verification is available if MMUI is installed on your system. It works like a personal verification for network sites. You record the site name verification from the administration terminal. It is used to confirm the site name when a message is addressed or when users receive a message from a network site.

For more information, refer to the *Meridian Mail Compact Option Enterprise Networking Installation and Administration Guide* (NTP 555-7001-222).

Procedure

To record a site name verification, follow these steps.

Starting Point: The Main Menu

Step Action

-
- 1 Select Network Administration.
 - 2 Select the type of networking administration.
 - 3 Select the type of site maintenance.
 - 4 Select the [Add] softkey for a new site or the [View/Modify] softkey for an existing site.
 - 5 Select the [Voice] softkey.
Result: The current screen remains displayed; the softkey display changes to [Cancel].
The system prompts for an extension number.
 - 6 Type the extension number of the telephone set you will use to make the recording, and press <Return>.
Result: The phone rings.
 - 7 Pick up the telephone handset.
Result: The system displays the recording softkeys.
 - 8 Select the [Record] softkey.
Result: The system displays the [Stop] softkey in place of the [Record] softkey.
You hear a tone through the telephone receiver.
 - 9 At the tone, begin speaking into the receiver.
Note: Recording stops automatically if the recording exceeds the Maximum Prompt Size or the Record Timeout set in the Voice Services Profile.
 - 10 To stop recording, select the [Stop] softkey.
Result: The recording stops automatically, and the system again displays the recording softkeys.

Step Action

- 11 Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11.
delete the recording	go to step 14.
record the verification again	go to step 7.
save the recording	go to step 18.

- 12 To review your recording, select the [Play] softkey.

Result: The system plays the recording.

The system displays the [Stop] softkey.

- 13 To stop the playback at any time, select the [Stop] softkey.

Result: The system again displays the recording softkeys.

- 14 To delete the recording, select the [Delete] softkey.

Result: The system displays the [OK to Delete] and [Cancel] softkeys.

You are requested to confirm the deletion.

- 15 Use the following table to determine the next step.

IF you want to	THEN
cancel the deletion	go to step 15.
confirm the deletion	go to step 16.

- 16 To cancel the deletion, select the [Cancel] softkey.

Result: The recording is not deleted.

The system again displays the recording softkeys.

Step	Action
------	--------

- | | |
|----|---|
| 17 | <p>To delete the recording, select the [OK to Delete] softkey.</p> <p>Result: The system deletes the recording.</p> <p>The system again displays the recording softkeys.</p> |
| 18 | <p>To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone.</p> <p>Result: The system displays the original softkeys.</p> <p>Note: When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey.</p> <p>When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.</p> |
| 19 | <p>To update the screen and store the changes to the recording, use the [Save] softkey.</p> |

Recording a personal verification for the broadcast mailbox

Introduction

This topic provides information and procedures for recording a personal verification for the broadcast mailbox.

You can record a personal verification for the broadcast mailbox so that when you enter the mailbox number during message composition, you get a verification that you have entered the correct number.

The personal verification for a broadcast mailbox can say something like: *"Broadcast mailbox 5555."*

To set up a broadcast message, a special mailbox number (the broadcast mailbox number) is defined in the Voice Messaging Options screen.

When you compose a broadcast message, you specify the broadcast mailbox number, and all users on the system receive your message.

Recording from the administration terminal

To record a personal verification for the broadcast mailbox from the administration terminal, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Messaging Options.
3	Move the cursor to the Broadcast Mailbox Personal Verification Recorded (Voice) field.
4	Select the [Voice] softkey.

Result: The system prompts you for a phone number in dialable format.

Step Action

- 5 Type the extension of the phone you will use to record the verification, and press <Return>.
Result: The phone rings.
- 6 Pick up the receiver.
Result: The recording softkeys are displayed.
- 7 Select the [Record] softkey.
Result: The system displays the [Stop] softkey in place of the [Record] softkey.
You hear a tone through the telephone receiver.
- 8 At the tone, say the verification.
Example: "Broadcast mailbox 5555."
- 9 To stop recording, select the [Stop] softkey.
Result: The recording stops automatically, and the system again displays the recording softkeys.
- 10 Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11 .
save the recording	go to step 13 .
rerecord the recording	press the [Delete] key, and go to step 7 .
- 11 To play back the recording, select the [Play] softkey.
Result: The system plays the recording.
The system displays the [Stop] softkey.

Step Action

- 12 To stop the playback at any time, select the [Stop] softkey.
Result: The system again displays the recording softkeys.
- 13 To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone.
Result: The system displays the original softkeys.
Note: When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey.
When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
- 14 To update the screen and store the changes to the recording, use the [Save] softkey.
-

Recording and sending broadcast messages

Introduction

This topic explains how you and the users on your system can record and send broadcast messages using the telephone handset.

Definition: broadcast message

A broadcast message is a message that is sent to all Meridian Mail Compact Option users. When you or the users on your system compose a message to the broadcast mailbox, the message is sent to all users on the system.

Setting up a broadcast mailbox

To set up a broadcast mailbox, you assign a mailbox number to the broadcast mailbox in the Voice Messaging Options screen. You do not need to set up an actual mailbox through User Administration. For more information about setting up broadcast mailboxes, see Chapter 19, "Voice messaging options".

Composing and sending broadcast messages

Any user who knows the broadcast mailbox number and has access to a mailbox with broadcast capability can also compose and send broadcast messages. It is recommended that users try to avoid sending broadcast messages during busy hours.

Procedure

To record and send a broadcast message, follow these steps.

Step	Action
1	Log on to a Meridian Mail Compact Option mailbox with broadcast capability.
2	Press 75 , enter the broadcast mailbox number (the default is 5555), and press # , twice .
3	To start recording, press 5 .
4	At the tone, record your broadcast message.
5	To stop recording, press # .

Step Action

- | | |
|---|--|
| 6 | To check your broadcast message, press 2 . |
| 7 | To send the broadcast message, press 79 . |
| 8 | To end your voice messaging session, press 83 , and then hang up. |
-

Making Voice Services recordings

Introduction

The Voice Services feature enables you to create custom call answering applications. Voice services recordings include announcement recording, Thru-Dial greetings, voice menu greetings, voice menu choices, and voice menu prompts.

This topic provides an overview of making Voice Services recordings.

Announcements

This service enables you to record messages that can be played back within a voice menu or as a stand-alone service that can be dialed directly by a caller.

Thru-Dial services

These services access predefined DN's or user-prompted DN's that can be used within a voice menu service or as a separate service with a directory number. Thru-Dial services can be created to provide a variety of dialing options to users of Meridian Mail Compact Option.

Voice Menus

The Voice Menus service enables you to create single-layered or multilayered menus that present choices to callers. Callers make their selections by pressing the key on the telephone keypad that corresponds to the action they wish to perform.

Voice Prompt Maintenance

This service enables you to modify the prompts and greetings available in your voice menus and announcements using a telephone.

Procedure

To make a Voice Services recording, follow these steps.

Starting Point: The Main Menu

Step Action

- 1 Select Voice Administration.
- 2 Select Voice Services Administration.
- 3 Select the type of voice service.
- 4 Use the following table to determine the next step.

IF you want to	THEN
create a new Voice Service recording	select the [Add] softkey.
add a new voice recording to an existing voice service	select the [View/Modify] softkey.
modify an existing voice recording	select the [View/Modify] softkey.

- 5 Use the following table to determine the next step.

IF you want to make	THEN move the cursor to the
an Announcement recording	Announcement Recorded field.
a Thru-Dial recording	Greeting Recorded field.
a Voice Menu recording	Greeting Recorded field or Menu Choices Recorded field.

- 6 Select the [Voice] softkey.
- 7 Type the extension of the phone you will use to make the recording, and press <Return>.

Result: The phone rings.
- 8 Pick up the receiver.

Result: The recording softkeys are displayed.
- 9 Select the [Record] softkey.

Result: The system displays the [Stop] softkey in place of the [Record] softkey.

You hear a tone through the telephone receiver.

Step Action

- 10 At the tone, make your recording.
 - 11 To stop recording, select the [Stop] softkey.
Result: The recording stops automatically, and the system again displays the recording softkeys.
 - 12 Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 13 .
save the recording	go to step 15 .
rerecord the recording	press the [Delete] key, and go to step 9 .
 - 13 To play back the recording, select the [Play] softkey.
Result: The system plays the recording.
The system displays the [Stop] softkey.
 - 14 To stop the playback at any time, select the [Stop] softkey.
Result: The system again displays the recording softkeys.
 - 15 To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone.
Result: The system displays the original softkeys.
Note: When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey.
When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
 - 16 To update the screen and store the changes to the recording, use the [Save] softkey.
-

Chapter 6

Setting up Meridian Mail Compact Option security

In this chapter

<u>Overview</u>	<u>6-2</u>
<u>Section A: Telecommunication criminals and the problems they pose</u>	<u>6-3</u>
<u>Section B: Using Basic Access Restrictions features</u>	<u>6-9</u>
<u>Section C: Features that modify access restrictions</u>	<u>6-21</u>
<u>Section D: Controlling remote access to calling privilege</u>	<u>6-45</u>
<u>Section E: Controlling access through Least Cost Routing (BARS/NARS)</u>	<u>6-53</u>
<u>Section F: Controlling access to PBX administration programs</u>	<u>6-85</u>
<u>Section G: Controlling Direct Inward System Access</u>	<u>6-95</u>
<u>Section H: Restriction/Permission lists</u>	<u>6-101</u>
<u>Section I: Controlling access to Meridian Mail Compact Option services and features</u>	<u>6-115</u>
<u>Section J: Controlling access to Meridian Mail Compact Option mailboxes</u>	<u>6-131</u>
<u>Section K: Monitoring access to Meridian Mail Compact Option mailboxes and features</u>	<u>6-161</u>
<u>Section L: Equipment security</u>	<u>6-177</u>

Overview

Introduction

In today's telecommunications environment, every computerized system is potentially open to unauthorized access. As system administrator, it is your responsibility to take all necessary precautions to prevent security breaches. For example, unless your system has been properly secured, someone who is connected to Meridian Mail Compact Option (such as a user who is logged on to a mailbox, or an external caller who has connected to Meridian Mail Compact Option through a call answering session or a voice menu) can place unauthorized calls that will be billed to your system.

In this chapter

This chapter is divided into

- an overview which describes the purpose and contents of this chapter
- Section A which describes the types of telecommunication criminals and the problems they pose to your system
- a third part which provides information and instructions on how you can use Meridian Mail Compact Option software features to control access to your switch
This part starts at [Section B](#) and ends at [Section H](#).
- a fourth part which provides information and instructions on how to use Meridian Mail Compact Option security features
This part starts at [Section H](#) and ends at [Section K](#).
- Section L which describes how to control access to your system hardware

Section A **Telecommunication criminals and the problems they pose**

In this section

[Overview](#) [6-4](#)

[Designing a security system](#) [6-7](#)

[Ongoing security measures](#) [6-8](#)

Overview

Introduction

Telecom fraud has existed since the 1970s when “telephone criminals,” or hackers, called their families and friends using stolen credit calling codes. By the late 1970s, hackers were using modems to access computerized systems from remote locations. By the mid-1980s, they were able to crack codes at computer speed using a personal computer with random number generating programs and autodialers.

Today, telephone operating companies are no longer the primary target for toll fraud as these companies have decreased their vulnerability by aggressively using software controls and prosecuting toll fraud criminals. For this reason, hackers trying to steal codes have migrated to new and potentially more devastating targets—customer premise equipment (for example, the PBX, Meridian 1 Option 11C Compact, and so on). Hackers are now using PBXs to place thousands of unauthorized calls primarily through inbound 800 numbers and voice mail.

What they gain

Hackers are usually after one of the following:

- authorization codes which allow them to use your private branch exchange (PBX) for local and long-distance calls
Authorization codes can then be sold or stored for future use.
- the use of your voice messaging system for their own purposes
For example, they can use your system as a bulletin board to exchange lists of calling card numbers, coordinate illegal activities, and so on.
- the degradation of your system performance

How they do it

There are several ways in which a hacker can try to access your system. The first is unauthorized access to the PBX; the second is unauthorized access to the voice messaging system, in this case, Meridian Mail Compact Option; unauthorized access to personal mailboxes; and unauthorized access to the equipment.

Therefore, a good security system has to incorporate elements from PBX and system security, and awareness on the part of your users in order to provide effective security.

Unauthorized access to the PBX

Hackers are using the PBX to place unauthorized calls primarily through inbound 800 numbers and voice mail.

Nortel's Meridian 1 Option 11C Compact product meets a wide variety of customer requirements. In particular, the Option 11C Compact has security features to help minimize its vulnerability while maintaining its flexibility.

For more information, see Sections B to G.

Unauthorized Meridian Mail Compact Option access

Hackers may attempt to hack into your voice messaging system so they can use the outdialing feature to make free local- and long-distance calls.

With Meridian Mail Compact Option, you can reduce, if not eliminate, this abuse by implementing some or all of the recommendations for system access. For more information, see Sections H to K.

Unauthorized mailbox access

Most hackers want access to the outdialing features—they are not concerned with personal mailboxes. If they do hack into a personal mailbox, they usually have some “fun” with it like changing the greeting, listening to messages, and so on.

With Meridian Mail Compact Option, you can reduce the risk of unauthorized mailbox access by implementing some or all

of the recommendations for mailbox access. For more information, [see “Controlling access to Meridian Mail Compact Option mailboxes” on page 6-131.](#)

Unauthorized access to the equipment

Your system hardware could be a potential point of unauthorized access.

What can be done about it?

Inadequate control of calling privileges and of physical access to switching systems can cost your business millions of dollars. To secure your PBX and limit its exposure to corporate espionage and toll fraud, you need to implement security measures for

- PBX access
- Meridian Mail Compact Option system access
- personal mailbox access
- equipment access

Designing a security system

Introduction

When designing a security system, consider the following two questions:

- How can you train your staff to responsibly use Meridian Mail Compact Option?
- How can you prevent unauthorized use of your PBX and Meridian Mail Compact Option system?

Both of these factors will help in keeping your Meridian Mail Compact Option system safe from individuals who want to abuse your system.

Training your staff

Controlling access privileges to prevent PBX toll fraud and abuse of your telephone system will affect *all* employees in your organization, regardless of their positions or responsibilities. Implementing a communication program about the potential for fraud and abuse of your Meridian Mail Compact Option communication system will help motivate your employees to prevent such abuse.

Ongoing security measures

Introduction

Once you have established your security practices, you should review them

- several months after the practices have been implemented so you can evaluate the results

This will help determine if certain practices require modification.

- whenever you notice strange calling patterns

These patterns will appear on reports listing numbers that are being called from your location or charges that are being billed to your company.

Remember to include your security practices in the orientation session for new employees.

Section B **Using Basic Access Restrictions features**

In this section

<u>Overview</u>	<u>6-10</u>
<u>Trunk Group Access Restrictions</u>	<u>6-11</u>
<u>Class of Service</u>	<u>6-13</u>
<u>TGAR/TARG and CLS interaction</u>	<u>6-18</u>
<u>Transfer feature on modems</u>	<u>6-17</u>

Overview

Introduction

By providing internal and external users access only to the facilities and calling privileges that their jobs require, you can greatly decrease the potential for system abuse and toll fraud. With Basic Access Restrictions features, you can deter internal abuse and restrict external access to toll facilities.

The features

The Basic Access Restrictions features you can apply to stations, TIE trunks, and authorization codes are as follows:

- **Trunk Group Access Restrictions (TGAR/TARG)** controls the specific trunk groups to which a station, TIE trunk, Direct Inward System Access (DISA) directory number, or authorization code has direct access.

For more information, [see “Trunk Group Access Restrictions” on page 6-11.](#)

- **Class of Service (CLS)** controls the degree of access; that is, once access is provided, CLS determines whether users can make local, TIE trunk, or long-distance calls.

For more information, [see “Class of Service” on page 6-13.](#)

Trunk Group Access Restrictions

Introduction

Trunk Group Access Restrictions (TGAR) controls access to various trunk groups including trunks that interface with the exchange network, with TIE and CCSA networks, and with services such as paging, dictation, and recorded announcements.

How it works

Stations, TIE trunks, DISA directory numbers (DNs), and authorization codes are assigned to a group (TGAR). When users attempt to access a trunk route from a station, TIE trunk, DISA DN, or authorization code, the software compares their group assignment (TGAR) against the list of denied Trunk Access Restrictions Group (TARG) associated with the trunk route they are trying to access.

If access is permitted, the Option 11C Compact software then uses the Class of Service (CLS) assignment to determine call eligibility. The system always uses the most restrictive assignment (CLS or TGAR) to determine call eligibility when a user is trying to access trunk facilities directly.

By partitioning stations, TIE trunks, DISA DNs, and authorization codes into appropriate groups within the business, you can stem internal abuse and external fraudulent activity, such as “looping” from PBX to PBX or to other carriers to mask the call’s origin.

Implementing and auditing the feature

Use the following table to implement or audit the TGAR/TARG feature on the Option11C Compact.

For	Implement using	Print using
Stations	LD 10/11—TGAR	LD 20 by TNB LD 10/11 by TN
Authorization codes	LD 88—TGAR	LD 88 by authorization code
TIE trunks	LD 14—TGAR	LD 20 by TNB
Trunk groups (Route)	LD 16—TARG	LD 21 by route or access code
DISA DN's	LD 24—DISA	LD 24 by DISA DN

Class of Service

Introduction

Class of Service provides the flexibility to partition stations, TIE trunks, DISA DN's, and authorization codes into calling privilege "levels". Again, these features can inhibit internal abuse and help protect your system by preventing users from placing calls through external sources.

Class of Service restriction levels

You can assign any one of the following Class of Service restriction levels to each station, TIE trunk, and authorization code to control the degree of access to the exchange network.

- ***Unrestricted Service (UNR)*** Allowed to originate and receive calls from the exchange network.
- ***Conditionally Unrestricted (CUN)*** Allowed to receive calls from the exchange network. Considered toll-denied for calls placed through direct access to trunk but unrestricted for toll calls placed through Automatic Number Identification (ANI).
- ***Conditionally Toll-Denied (CTD)*** Allowed to receive calls from the exchange network. Considered toll-denied for calls placed through direct access to trunks, but unrestricted for toll calls placed through Basic/Network Alternate Route Selection (BARS/NARS).
- ***Toll-Denied Service (TLD)*** Allowed to receive calls from the exchange network and to dial local exchanges. Calling privileges of toll-denied stations may be modifiable through Code Restriction or New Flexible Code Restriction to allow or deny certain dialing sequences.
- ***Semi-Restricted Service (SRE)*** Allowed to receive calls from the exchange network. Restricted from all dial access to the exchange network but allowed access

to TIE trunks. Allowed to access the exchange network through an attendant or an unrestricted station.

- ***Fully Restricted Service*** Three classes of Fully Restricted Service are available:
 - ***FRE*** Allowed to originate and receive internal calls. Allowed access to TIE and CCSA networks, and to and from the exchange network using call modification from an unrestricted station. Denied access, either through dialing or through the attendant, to and from the exchange network.
 - ***FRI*** Allowed to originate and receive internal calls. Allowed access to TIE and CCSA networks. Denied access to and from the exchange network.
 - ***FR2*** Allowed to originate and receive internal calls. Denied access to TIE and CCSA networks, and to the exchange network.

Assigning a Class of Service

The following table outlines various call types and indicates whether they are possible within each Class of Service assignment.

	Class of Service assignment						
Call type	UNR	CTD/CUN	TLD	SRE	FRE	FR1	FR2
Incoming trunk calls	Yes	Yes	Yes	Yes	Through call modification only (see Note 1)	No	No
Outgoing non-toll trunk call	Yes	Yes	Yes	Attendant or station-extended only	Station-extended only	No	No
Outgoing toll trunk call (see Note 2)	Yes	No direct access. Yes, through BARS, NARS, or CDP if allowed through NCOS	Attendant or station-extended only		Attendant or station-extended only	No	No
Incoming/outgoing TIE call	Yes	Yes	Yes	Yes	Yes	Yes	No
Station-to-station call	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Note 1: Call modification (transfer from station, call pickup, or transfer answer from any station) may be allowed or denied for each system.							
Note 2: A toll call to the Option11C Compact is 0+ or 1+ dialing on a central office or foreign exchange trunk.							

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Class of Service feature.

For	Implement using	Print using
Stations	LD 10/11—CLS	LD 20 by TNB; LD 10/11 by TN LD81 by COS
Authorization codes	LD 88—CLS	LD 88 (by authorization code)
TIE trunks	LD 14—CLS	LD 20 by TNB
Trunk groups (Route)	LD 24—CLS	LD 24 (by DISA DN)

Transfer feature on modems

Introduction

Hackers also use “smart” modems to infiltrate a PBX taking advantage of systems whose 2500 dataports were programmed with unnecessary features. The most common data hack is perpetrated by one “smart” modem calling another and leaving a series of instructions at the receiving modem.

How it works

The instructions require the receiving modem to emulate a switchhook flash (transfer), out pulse a series of numbers from the calling modem, and switchhook again. This effectively transfers the call back to the PBX and out again.

What you can do about it

The modem port usually has calling privileges assigned that are not required for the modem to function. Many times, a 2500-set template is used that is also used for single-line phones. Frequently, the administrator is unaware that the 2500 port will be used for data,

Modem phones should be identified and the transfer feature removed if possible. The default on 2500 sets is “deny.” Be sure the class of service, TGAR, and NCOS do not allow long-distance calling whenever possible.

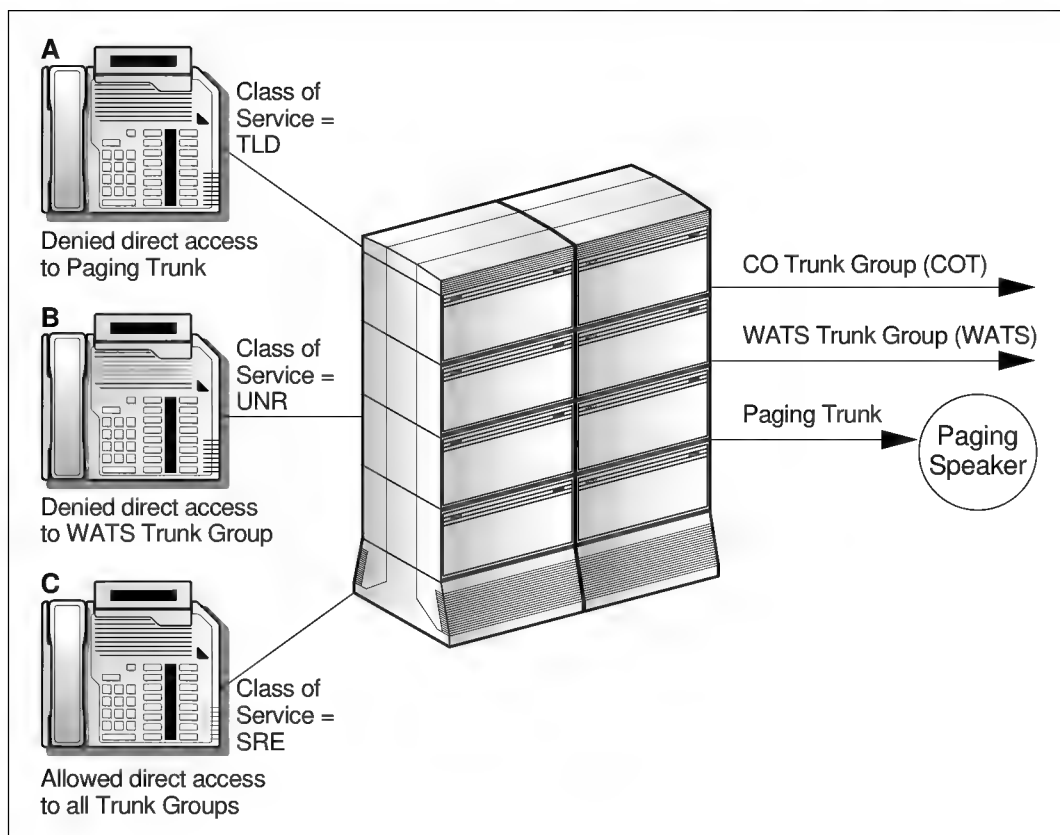
TGAR/TARG and CLS interaction

Introduction

You can use CLS and TGAR/TARG to control access to and from your trunk facilities. By assigning the most appropriate Class of Service (COS) and TGAR, you can limit your system's vulnerability to toll fraud and internal abuse.

Interaction

The following illustration shows the interaction between the Class of Service (CLS) assignment and Trunk Group Access Restrictions (TGAR).



G100446

Interaction (cont'd)

In this illustration, the following occurs:

- User C dials access code to CO trunk group, followed by 555-6100.
- Option11C Compact checks Trunk Access Restriction Group to see if user has access to CO trunks. User C does.
- Option11C Compact checks CLS (SRE) to see if user can make a local call.

User C cannot make a local call.

- Call is not allowed through CLS.

In summary, when a user attempts to access a trunk route, the Option11C Compact compares the TGAR assignment against the list of denied TARGs associated with the route that the user is trying to access. If the TARG is not listed, the Option11C Compact then uses the CLS assignment to determine call eligibility.

The system uses the most restrictive assignment, CLS or TGAR, to determine call eligibility when a user is attempting to place a call by way of direct access to trunk facilities.

Section C **Features that modify access restrictions**

In this section

<u>Overview</u>	<u>6-22</u>
<u>System Speed Call</u>	<u>6-24</u>
<u>Authorization Codes</u>	<u>6-26</u>
<u>Station Specific Authorization Codes</u>	<u>6-28</u>
<u>Forced Charge Account</u>	<u>6-30</u>
<u>Controlled Class of Service</u>	<u>6-33</u>
<u>Enhanced Controlled Class of Service</u>	<u>6-36</u>
<u>Flexible Feature Codes—Electronic Lock</u>	<u>6-37</u>
<u>Code Restriction</u>	<u>6-39</u>
<u>New Flexible Code Restriction</u>	<u>6-42</u>

Overview

Introduction

The following features can be used to selectively override Class of Service (CLS) and Trunk Group Access Restrictions (TGAR) when you need to extend a station's or TIE trunk's normal calling capabilities:

- System Speed Call
For more information, [see "System Speed Call" on page 6-24.](#)
- Authorization Code
For more information, [see "Authorization Codes" on page 6-26.](#)
- Station Specific Authorization Code
For more information, [see "Station Specific Authorization Codes" on page 6-28.](#)
- Forced Charge Account
For more information on, [see "Forced Charge Account" on page 6-30.](#)
- Controlled Class of Service
For more information, [see "Controlled Class of Service" on page 6-33.](#)
- Enhanced Controlled Class of Service
For more information, [see "Enhanced Controlled Class of Service" on page 6-36.](#)
- Flexible Feature Codes—Electronic Lock
For more information, [see "Flexible Feature Codes—Electronic Lock" on page 6-37.](#)
- Code Restrictions
For more information, [see "Code Restriction" on page 6-39.](#)
- New Flexible Code Restriction

For more information, [see “New Flexible Code Restriction” on page 6-42.](#)

System Speed Call

Introduction

System Speed Call extends the capabilities of the Speed Call feature. In addition to providing abbreviated dialing, using an entry in a System Speed Call list lets the internal user temporarily override the Class of Service and TGAR assigned to a station, and place a call to a telephone number in the System Speed Call list.

How it works

With this feature, you can assign the most appropriate CLS and TGAR restrictions to a station to limit the potential for unauthorized calling, and, at the same time, allow calls to approved destinations. The “approved telephone numbers” that you define in a system Speed Call list extend the station’s calling privileges beyond the station restriction levels.

You can assign stations to different System Speed Call lists. You can also designate these stations as either System Speed Call Users (SSUs) or System Speed Call User/Controllers (SSCs) of the list. You can also assign list controlling capabilities to a key on the attendant console. However, this key cannot override CLS and TGAR because the attendant is not subject to these restrictions.

Note: A System Speed Call list can also override the station restrictions imposed through the Least Cost Routing software.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the System Speed Call feature.

For	Implement using	Print using
Stations	LD 10—FTR LD11—SSU, KEY	LD 20 by TNB; LD 10/11 by TN LD81 by SSU, SSC, KEY
Speed Call list	LD 18—SSC, all prompts	LD 20 by list number
Attendant	LD 12—KEY	LD 20 by TNB

Authorization Codes

Introduction

Authorization codes allow users to place business calls from stations normally restricted from doing so. These restricted stations may be located in areas of public access or used by employees who do not require broader calling privileges.

How it works

Authorization codes enable selected users to temporarily override the access restrictions assigned to a station or a TIE trunk. A user enters an authorization code which has an associated Class of Service (CLS), TGAR, and Least Cost Routing or Network Class of Service (NCOS). The user has the calling privileges of the authorization codes rather than those of the station or TIE trunk for the duration of the call.

Considerations

When you implement the Authorization Code feature, you should consider making the authorization codes as long as your business will allow, assigning unique authorization codes to each user, and allowing calling privileges based on user requirements.

You can also output the codes as part of the Call Detail Records (CDR) to look for call patterns that indicate possible unauthorized access or abuse. You should design and implement procedures for assigning authorization codes to new employees and for deleting codes that are no longer valid because of attrition or abuse.

Note: You may use authorization codes to override the station restrictions imposed through the Least Cost Routing software.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Authorization Codes feature.

For	Implement using Overlay programs/features prompts	Print using Overlay programs
Authorization codes	LD88—all prompts	LD 88 by authorization code

Station Specific Authorization Codes

Introduction

The Station Specific Authorization (Authcode) Code is offered as a separate package. It allows you to define the authorization code access level of a set.

How it works

The Station Specific Authorization Code feature is implemented on a per set basis. The system will cross-check between overlays 10, 11, and 88 to ensure that the authorization code being used is valid. The only time cross-checking is not performed is when authorization codes are deleted from overlays 10 or 11. You must remove the authorization codes from overlay 88 as well as overlays 10 or 11.

Levels of access

There are three levels of authorization code access:

- ***Authcode Unrestricted (AUTU)*** A set programmed AUTU will be allowed to enter any authorization code without additional restrictions.
- ***Authcode Restricted (AUTR)*** When a set is configured AUTR, the authorization code entered by the user must match one of the preassigned authorization codes. Any other authcode will be treated as invalid, and an error message will be generated at the TTY.
- ***Authcode Denied (AUTD)*** No authorization code entry will be accepted for a set configured as AUTD.

Implementing and auditing

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Station Specific Authorization Codes feature.

For	Implement using	Print using
LD 10/11 stations	LD 10/11 (AUTU), AUTR, AUTD MAUT YES/NO SPWD (prompted if MAUT=YES) AUTH	LD 20 by TNB LD 10, 11 by TNB
LD 81 ODAS	LD 81 FEAT AUTU, AUDT, AUTD	LD 81 by FEAT
LD 88 Authorization Code	LD 88 AUTH	LD 88 by AUTH

Forced Charge Account

Introduction

With Forced Charge Account (FCA), the system forces the user to act before greater calling privileges are granted.

How it works

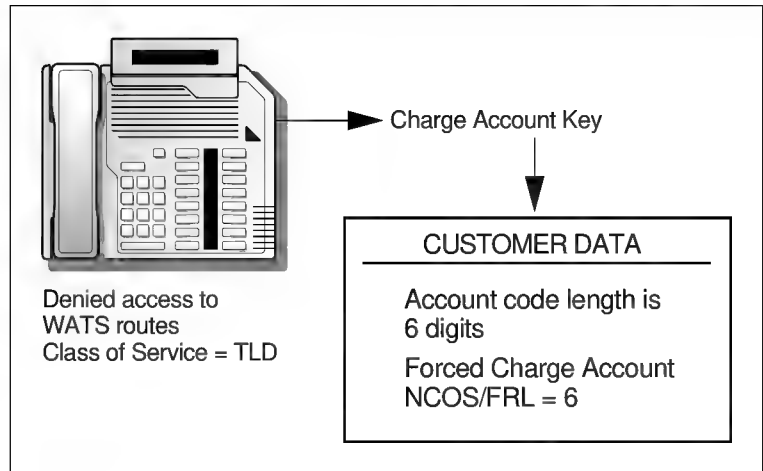
The Forced Charge Account feature temporarily overrides the toll-denied Class of Service Restriction (TLD) provided the user enters an account code before placing a toll call. After the user enters an account code, the Option11C Compact software checks only for a valid account code length—not for valid digits within an account code. Once the Option11C Compact verifies the account code length, the user has an unrestricted Class of Service or the customer-defined Forced Charge Account Network Class of Service (NCOS), or both, for the duration of the call.

The Call Detail Recording (CDR) software outputs a charge record which identifies the charge account used for the call.

Note: You can use the Forced Charge Account feature to override the restrictions imposed through the Least Cost Routing software.

Example

The following illustration is an example of how Forced Charge Account works.



G100450

Example, cont'd

In this example, the following takes place:

- User goes off-hook to obtain a dial tone.
- User presses Charge Account key.
- User dials six-digit account code.
- Account code record is generated in CDR.
- User receives a dial tone and dials a number in the normal manner.
- Set becomes UNR (unrestricted) for this one call.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Forced Charge Account feature.

For	Implement using	Print using
Customer	LD 15—CHLN, FCAF, CHMN, FCNC	LD 21 by CDB or by CDR

6-32 Setting up Meridian Mail Compact Option security

For	Implement using	Print using
Stations	LD 10/11—TLD, FCAR	LD 10, 11 by TN LD 20 by TNB
TIE trunks	LD 14—TLD, FCAR	LD 20 by TNB

Controlled Class of Service

Introduction

You can use Controlled Class of Service to lower calling privileges of sets in unsecured areas and still raise their calling privileges when required. This feature is particularly effective in preventing internal abuse.

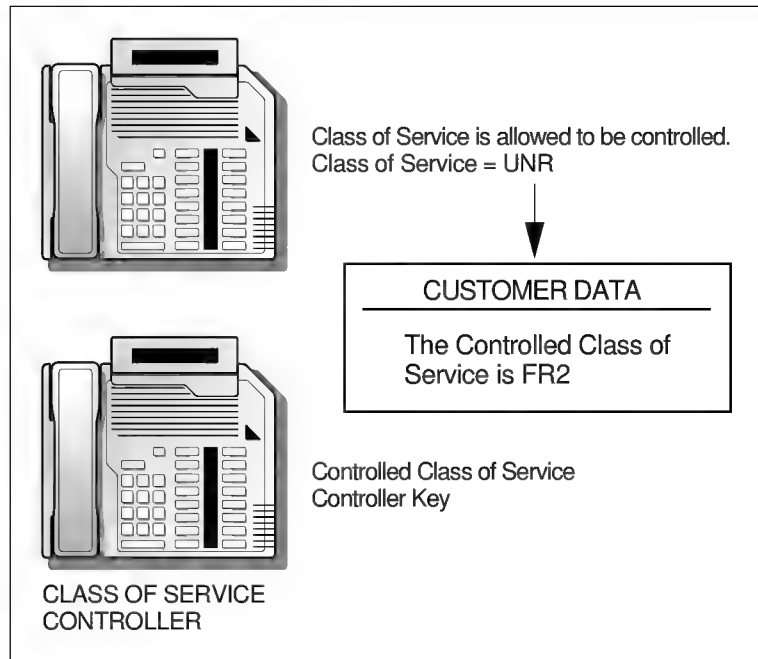
How it works

The Controlled Class of Service (CCOS) feature allows users of 2008 sets designated as controllers, and users of TTYs designated as background terminals, to temporarily alter a designated station's Class of Service assignments (CLS). When a station is in the controlled mode, its CLS is derived from the Controlled Class of Service restriction level defined for each customer.

Users of 2008 sets designated as controllers can place stations in a controlled mode one at a time whereas background terminals can alter individual, group, or all designated stations at one time.

Example

The following illustration is an example of how the Controlled Class of Service feature works.



G100451

In this example, the controller does the following

- Presses the Controller key.
- Dials the directory number of the set to be controlled.
- Presses the Controller key.

The set is now an FR2 Class of Service.

To return that set to the UNR Class of Service, the controller presses the Controller key, dials the DN for the set, and presses the Controller key again. The set will be reset to a UNR Class of Service.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Controlled Class of Service feature.

For	Implement using	Print using
Customers	LD 15—CCRS	LD 21 by CDB or by CCOS
Stations to be controlled	LD 10/11—CLS	LD 10, 11 by TN LD 20 by TNB
Stations to be controllers	LD 11—KEY	LD 20 by TNB LD 81 CCOS Key
Background terminals	LD 17—ADAN, USER	LD 22 by CFN, ADAN

Enhanced Controlled Class of Service

Introduction

This enhancement expands the Controlled Class of Service feature to further control calling privileges of stations in unsecured areas. Enhanced Controlled Class of Service (ECCS) extends the controller function of Controlled Class of Service (CCOS) to attendant consoles and the M3000 sets equipped with a Controller key. In addition, this enhancement allows for two more customer-defined levels of CCOS restriction.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Enhanced Controlled Class of Service feature.

For	Implement using	Print using
Customers	LD 15—CCRS, ECC1, ECC2	LD 21 by CDB or by CCOS
Stations to be controlled	LD 10/11—CLS	LD 10, 11 by TN LD 20 by TNB
Stations to be controllers	LD 11—KEY	LD 11 by TN LD 20 by TNB LD 81 CCOS Key
Attendants to be controllers	LD 12—KEY	LD 20 by TNB LD 81 CCOS key
Background terminals	LD 17—USER	LD 22 by CFN, by ADAN

Flexible Feature Codes—Electronic Lock

Introduction

Electronic Lock (ELK) allows selected users to activate and deactivate the Controlled Class of Service (CCOS) mode from their stations by entering the Station Control Password (SCPW) and the appropriate Electronic Lock code.

Station users can activate the Electronic Lock feature to prevent unauthorized calls from their sets when they are not able to control physical access. The feature is used typically in the evenings or on weekends.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Electronic Lock feature.

For	Implement using	Print using
Customers	LD 15-CCRS, SCPL	LD 21 by CDB or by FCR
Flexible Feature code	LD 57—FFCT, CODE, ELKA, ELKD	LD 57
Stations	LD 10/11—SCPW, CLS	LD 10/11 by TN LD 20 by TNB

Outgoing call barring

This feature permits a set user to restrict a phone to 1 to 3 levels of customer-defined calling restrictions. The user dials the OCBA, FFC, SCFW and OCB level desired. All subsequent calls from the station are screened through an NFRC table. Note that this feature can only increase calling restrictions. All other restricting features remain in effect.

Example:

OCB1 only allows calls to 911+internal calls

OCB2 allows calls to 911 and internal calls+local exchanges

OCB3 allows calls to 911, internal calls, local exchanges and attendant.

Used by the station owner when away from the station, especially for a prolonged period, or if the set is in a public place.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Outgoing Call Barring.

For	Implement using	Print using
Administration	LD 15 — NFCR, OCB1, OCB2, OCB3, SCPL LD 21 — by CDB or PCR LD 57 — FFCT, CODE, OCBA, OED LD 10/11 — SCPW, CLS-OCBA LD49 — FCR	LD 21 by CDB or PCR

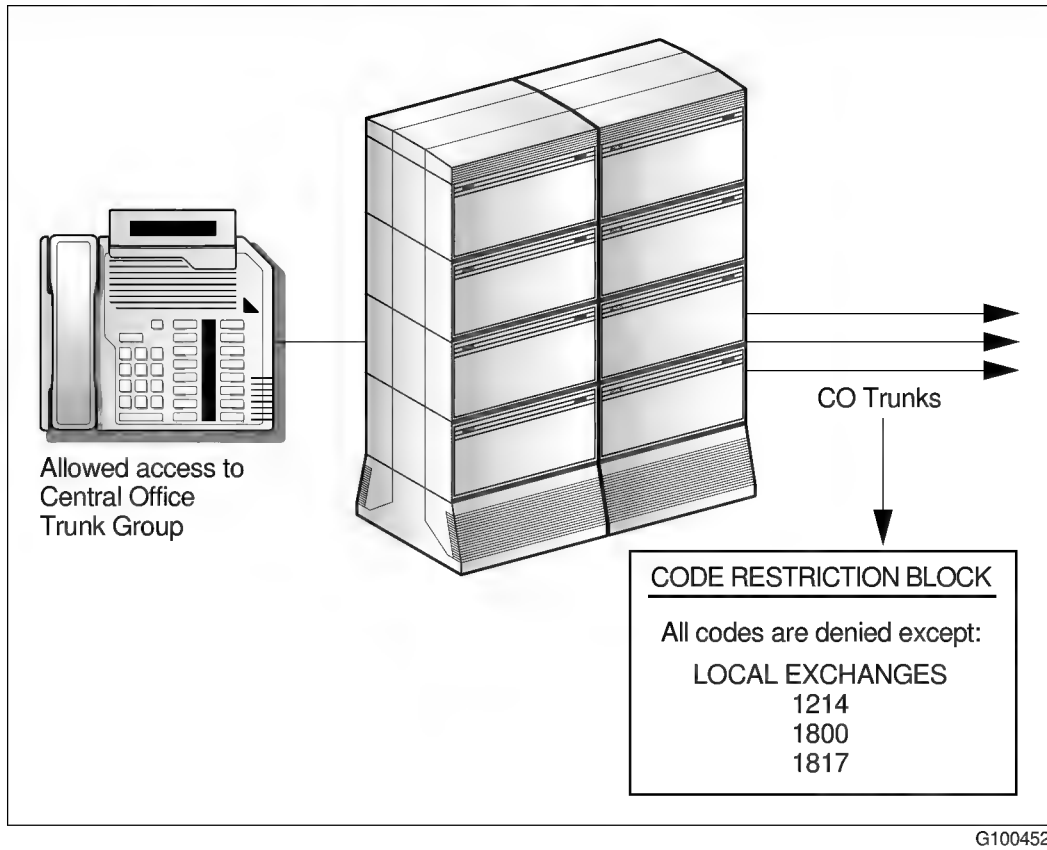
Code Restriction

Introduction

The Code Restriction feature allows toll-denied stations, TIE trunks, DISA DNs, and authorization codes limited access to the toll-exchange network—that is, to CO and FX trunks. For each CO and FX trunk group, you can build a code restriction block that specifies the allowed area codes and exchange codes for toll-denied users accessing those facilities.

Example

The following illustration is an example of how the Code Restriction feature works.



Example, cont'd

In this example, the following takes place:

- User goes off-hook and dials the access code for CO trunks followed by 1-800-555-0110.
- Station is TLD and not normally allowed to dial 1+, but a code restriction is in effect.
- Option11C Compact checks the Code Restriction Table for CO trunks and finds that 1-800 is allowed.
- The call is completed.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Code Restriction feature.

For	Implement using	Print using
Code Restriction	LD 19 all prompts	LD 21 by CRB
Stations	LD 10/11—CLS=TLD	LD 10/11 by TN LD 20 by TNB LD 81 by TLD

New Flexible Code Restriction

Introduction

To extend the calling privileges normally associated with toll-denied Class of Service, New Flexible Code Restriction allows you to partition toll-denied users into groups. Each toll-denied group can have unique calling privileges. New Flexible Code Restriction (NFCR) enhances Code Restriction by letting you selectively allow or deny toll-denied stations, TIE trunks, DISA DNs, and authorization codes to make certain calls on outgoing trunk routes. With New Flexible Code Restriction, the Option11C Compact determines whether the toll-denied user can make a call on a specific trunk route by checking the specific digit sequence dialed, the number of digits dialed, or both.

How it works

You can assign toll-denied users to a Network Class of Service (NCOS) and allow or deny calling privileges according to the Facility Restriction Level (FRL) of the NCOS. Toll-denied stations, TIE trunks, and authorization codes can be assigned from 1 to 100 possible NCOS groups. Each NCOS group can be assigned to one of eight possible FRLs.

When the toll-denied user accesses an outgoing route, the Option11C Compact compares the FRL of the user's NCOS to a table that defines the calling privileges associated with that trunk group.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the New Flexible Code Restriction feature.

For	Implement using	Print using
Customer	LD 15—NFCR, MAXT	LD 21 by CDB or by ESN
Network control	LD 87—NCOS, FRL	LD 87 by NCOS
New Flexible Code Restriction block	LD 49-FCR for all prompts	LD 49 FCR
Route	LD 16—FRL	LD 21 RDB
Station	LD 10/11—NCOS, CLS=TLD	LD 10, 11 by TN LD 20 by TNB LD 81 by COS, NCOS
DISA	LD 24—NCOS	LD 24 by DISA DN

Section D **Controlling remote access to calling privilege**

In this section

<u>Overview</u>	<u>6-46</u>
<u>Call Forward All Calls</u>	<u>6-47</u>
<u>Call Forward External Deny</u>	<u>6-48</u>
<u>Call Forward to Trunk Access Code—DID Calls</u>	<u>6-49</u>
<u>Internal Call Forward</u>	<u>6-50</u>
<u>User Selectable Call Redirection</u>	<u>6-51</u>

Overview

Introduction	Two of the most commonly abused features are Call Forward All Calls and Direct Inward System Access (DISA).
Call Forward	Call Forward is a convenient feature that allows users who are going to be away from their desks to forward their calls to another set or location.
Call Forward All Calls	The Call Forward All Calls feature is assigned on a per station basis and designates the maximum number of digits to which a user may call forward.
Direct Inward System Access	DISA allows users in remote locations to place calls through your corporate PBX.
Types of abuse	Station users have abused Call Forwarding by forwarding their sets to either a long-distance telephone number or to a trunk access code, then going offsite, and making a call to their sets. With the introduction of Remote Call Forward, non-users can abuse Call Forward if proper controls are not in place.
In this section	This section describes additional controls you can use with the Call Forward features to stem abuse and unauthorized calls.

Call Forward All Calls

Description

Call Forward (CFW) allows users to forward all calls manually to another number either internal or external to the system. The ability to forward a phone outside the system depends not only on the number of digits assigned to the call forward feature, but on the assignment of the feature Call Forward External Allow, also assigned on a phone-by-phone basis.

What you should look for

The default for CFW is 16, adequate for many international calls. Ensure this feature is restricted to the minimum in all cases (usually four—the standard number of digits in an extension). Be aware of the combinations of external forwarding and long digit strings allowed. Permit only where absolutely necessary.

How to use ICF

Ensure that Call Forward to Trunk Access Codes is set to “no” in the customer Data Block and that Call Forward External is denied. A combination of these features in the “allow” state would permit users to call forward their phones to BARS/NARS access codes or trunk access codes, and receive a second dial tone when looping through private networks or entering the system through DISA.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Call Forward All Calls feature.

For	Implement using	Print using
Stations	LD10, 11—CFW	LD 10, 11 by TN LD 20 by TNB LD 81 by CFW

Call Forward External Deny

Description

This feature provides the option to restrict, on a set-by-set basis, the ability to call forward all calls to an external directory number (DN).

The default value for Call Forward External becomes “deny.”

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Call Forward External Deny feature.

For	Implement using	Print using
Stations	LD 10, 11—CLS	LD 10, 11 by TN LD 20 by TNB LD 81 by CFXA, CFXD

Call Forward to Trunk Access Code—DID Calls

Description

You may not want your users to call forward their stations to an access code. After all, an unrestricted station forwarding to the central office trunk (COT) access code puts a whole world of calling capabilities at the caller's fingertips. Call Forward to Trunk Access Code provides you with the option to restrict, on a customer-by-customer basis, the ability to call forward direct in dial (DID) calls to a trunk access code.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Call Forward to Trunk Access—DID calls feature.

For	Implement using	Print using
Customer	LD 15—CFTA	LD 21 by CDB or RDR

Internal Call Forward

Description

Internal Call Forward (ICF) directs all internal calls to a specified location different from the call forward destination of external calls. An internal call is considered an extension-to-extension call, Direct Inward System Access (DISA) call, Group Call, a call over a trunk route designated as internal, an incoming trunk call using private numbering, or an attendant-originated call. The default for this feature is 4 digits but can be defined for up to 23 digits.

How to use ICF

Ensure that Call Forward to Trunk Access Codes is set to “no” in the customer Data Block and that Call Forward External is denied. A combination of these features in the “allow” state would permit users to call forward their phones to BARS/NARS access codes or trunk access codes, and receive a second dial tone when looping through private networks or entering the system through DISA.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Internal Call Forward feature.

For	Implement using	Print using
Customer	LD 15—CFTA	LD 21 by CDB or RDR
Stations	LD 10—FTR, ICF	LD 10, 11 by TN LD 20 by TNB LD 81 by ICF
Flexible Feature Codes	LD 57—ICFA, ICFD, ICFV	LD 57 by CODE

User Selectable Call Redirection

Introduction

This feature allows the user to select the destination for Forward No Answer, Busy Hunt, External Forward No Answer, and External Hunt. User Selectable Call Redirection is controlled by Flexible Feature Code, Special Prefix Code, or a User key on a multiline phone.

This feature requires a Station Control Password.

Ensure that the SCPW is unique for each phone with the feature allowed.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the User Selectable Call Redirection feature.

For	Implement using	Print using
LD 10/11 SETS	LD 10 SCPW, CLS, USRA	LD 10, 11 by TN, DN LD 20 by TNB LD 20 by DN
LD 15 CDB	LD 15 SPCL, FFCS	LD 21 by CDB, by CFW
LD 57 FFC	LD 57 USCR	LD 57 by CODE LD 81 by CODE

Section E **Controlling access through Least Cost Routing (BARS/ NARS)**

In this section

<u>Overview</u>	<u>6-54</u>
<u>Supplemental Digit Recognition</u>	<u>6-57</u>
<u>Supplemental Digit Restriction</u>	<u>6-60</u>
<u>Network Class of Service—Facility Restriction Level</u>	<u>6-63</u>
<u>Network Speed Call</u>	<u>6-68</u>
<u>Network Authorization Code</u>	<u>6-71</u>
<u>Authorization Code Conditionally Last</u>	<u>6-72</u>
<u>Time-of-Day Routing</u>	<u>6-75</u>
<u>Routing Control</u>	<u>6-78</u>
<u>Incoming Trunk Group Exclusion</u>	<u>6-81</u>

Overview

Introduction

Basic Alternate Routing System (BARS) and Network Alternate Routing System (NARS) software allows you to route outgoing calls over the least expensive facility available at the time the user places the call. You can use the BARS/NARS feature to prevent calls to a specific area code or exchange, or to international locations.

How BARS and NARS work

When the user dials an access code followed by the desired number, the software processes and routes the call. Based on the number the user dials, the Option11C Compact system reads a digit translation table. The translation determines which list of alternate routes the system will use to process the call. This list is called a route list index and contains alternate outgoing routes (trunk groups) for call completion.

Because the majority of toll-fraud calls terminate in the 809 area code and in international locations such as Egypt, Pakistan, and Columbia, consider not defining these codes in your translation tables if your business does not require that users call these locations. If you are required to make calls to destinations associated with fraud, you should consider assigning unique route list indexes to each of these destinations. Such a scheme provides the capability to assess normal call volumes and detect variations.

Assessment tools

Statistics are available to indicate the number of calls placed through each route list index. It is TFN001.

Available features

The following features are elements of BARS/NARS which allow you flexibility in restricting calling privileges:

- Supplemental Digit Recognition
- Supplemental Digit Restriction

**Available features,
cont'd**

- Network Class of Service—Facility Restriction Level
- Network Speed Call
- Network Authorization Code
- Authorization Code Conditionally Last
- Time-of-Day Routing
- Routing Control
- Incoming Trunk Group (TIE) Exclusion

**BARS/NARS features
to control access
privileges**

The following table lists the features you should consider implementing depending on the requirements of your business.

If your business requirement is to	Then we recommend you
totally deny an area code or a local exchange	do not define them in the translation table. Calls to those numbers attempted through BARS/NARS are blocked.
deny all access to certain country codes, or exchanges within an area code	use the Supplemental Digit Restriction feature or Translation Data Block. For more information, see “Supplemental Digit Restriction” on page 6-60.
inhibit the use of certain trunk groups	use the Network Class of Service (NCOS) Facility Restriction Level (FRL) and also (optionally) Trunk Group Access Restriction (TGAR) feature. For more information, see “Network Class of Service—Facility Restriction Level” on page 6-63 and “Trunk Group Access Restrictions” on page 6-11.
deny access to certain trunk groups or destinations at a specific time	use the Time-of-Day Routing feature. For more information, see “Time-of-Day Routing” on page 6-75.

If your business requirement is to	Then we recommend you
deny access to certain destinations after business hours, on weekends and holidays, or at other selected times.	use the Routing Control feature. For more information, see “Routing Control” on page 6-78.
deny calls to certain dialing sequences when those calls originate on TIE trunks	use the Incoming Trunk Group Exclusion. For more information, see “Incoming Trunk Group Exclusion” on page 6-81.

Supplemental Digit Recognition

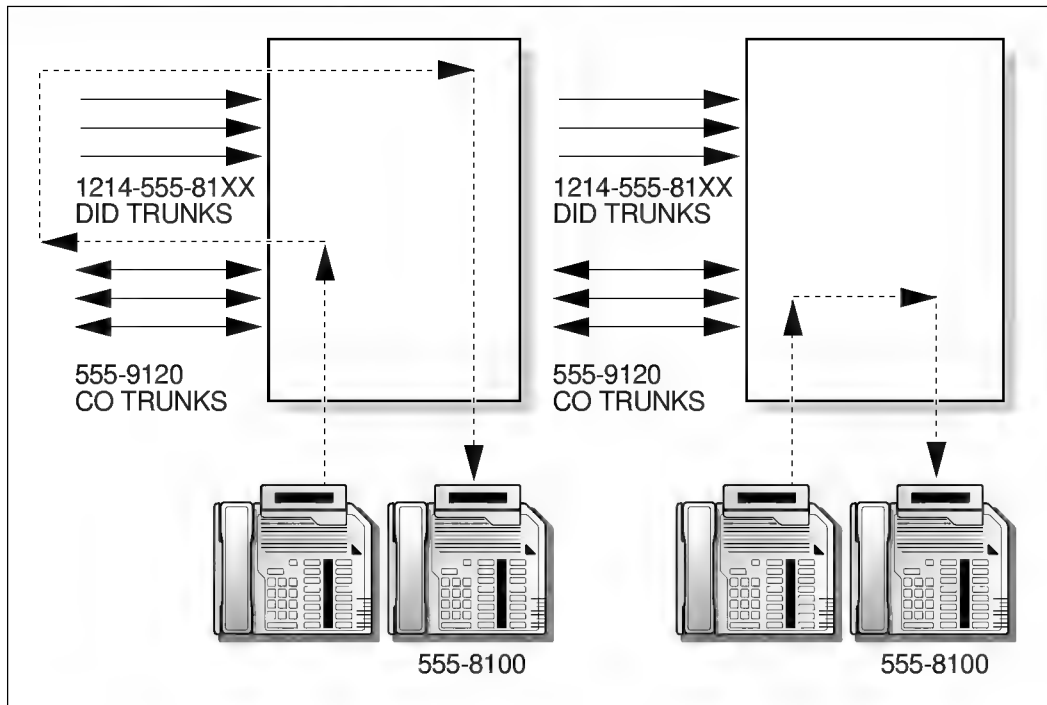
Description

One type of internal abuse or misuse occurs when callers use incoming TIE trunks. Callers on TIE trunks sometimes dial the BARS/NARS access code followed by the whole telephone number of an internal station.

When using Supplemental Digit Recognition, the Option11C Compact “recognizes” dialing sequences associated with internal calls, and thus prevents callers from using two trunks to complete an internal call.

Example

The following figure illustrates how the Supplemental Digit Recognition feature works.



G100453

Example, cont'd

In this example, the following takes place:

- User A dials 9-555-8100.
Option11C Compact is not programmed to recognize 555-8100 as an internal number.
The call is routed out over a CO trunk group and is returned to the Option11C Compact through the DID trunk group. An internal call now requires two trunks to be complete.
- User B dials 9-555-8100.
Option11C Compact is programmed to recognize 555-8100 as an internal number and deletes 555. Option11C Compact dials 8100. The call is completed internally.

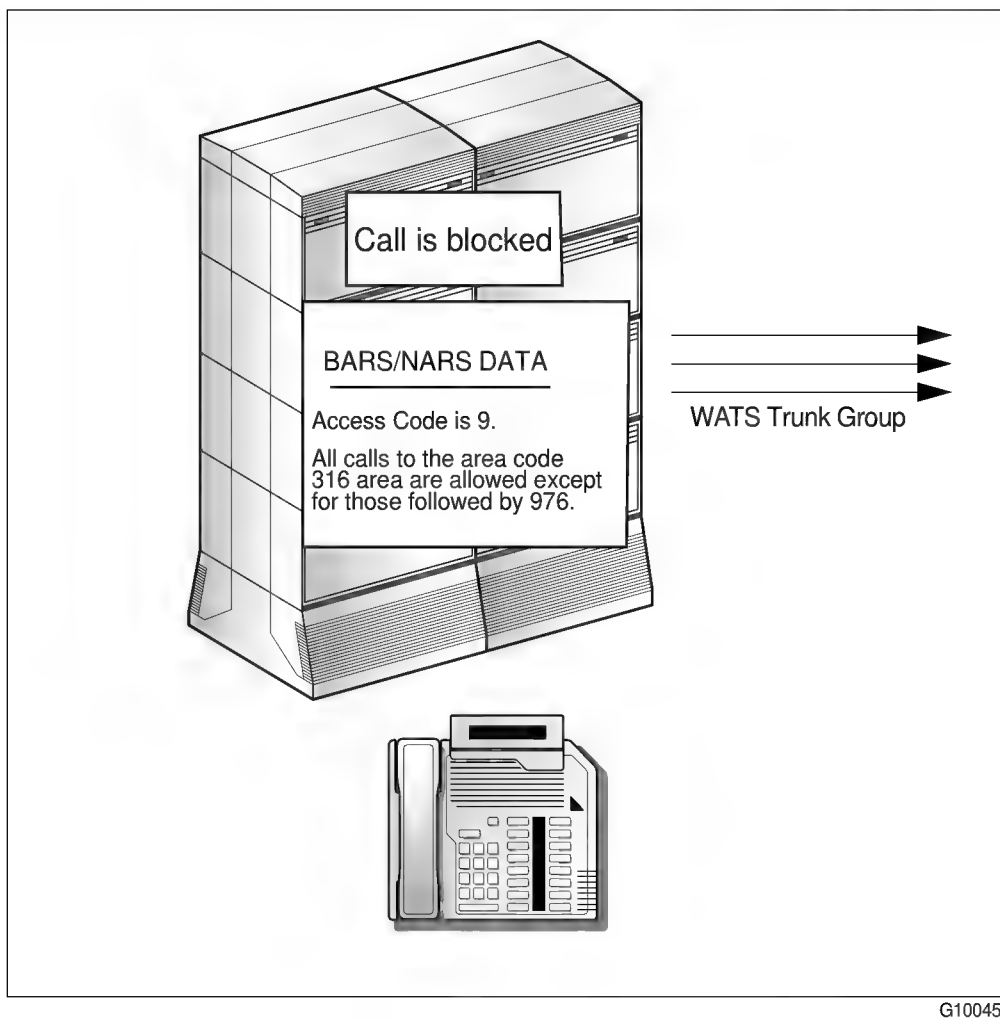
Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Supplemental Digit Recognition feature.

For	Implement using	Print using
ESN	LD 86—MXSD	LD 86 by FEAT=ESN
Network translation	LD 90—DENY, LDID, LDDD	LD 90 by NPA, NXX, or SPN

Supplemental Digit Restriction

Description	Because most toll-fraud calls are placed to international locations, you can use Supplemental Digit Restriction (SDR) to block calls to international locations that your users do not need to call.
How SDR works	Supplemental Digit Restriction enables you to block calls to certain telephone numbers within exchanges, area codes, or country codes. For example, you may have legitimate international calling requirements to many countries but none to those countries typically associated with fraud. Supplemental Digit Restriction lets you block calls to those countries.
Example	The following figure illustrates how the Supplemental Digit Restriction feature works.



In this example, the following takes place:

- The user dials 9-1-316-976-9090.
- The 9 triggers the Option11C Compact to use BARS/NARS data.

- Option11C Compact checks the Translation Table for 1316 and finds that 1316, followed by 976, is blocked.
- The call is blocked.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Supplemental Digit Restriction feature.

For	Implement using	Print using
ESN	LD 86—MXSD	LD 86 by FEAT=ESN
Network translation	LD 90—DENY, LDID, LDDD	LD 90 by NPA, NXX, or SPN

Network Class of Service—Facility Restriction Level

Description

A Network Class of Service (NCOS) designation is a group of calling privileges you can assign to a station, TIE trunk, DISA DN, or authorization code.

How NCOS works

The Entrepreneur system uses the NCOS to determine caller treatments and eligibility for outgoing calls that use the Least Cost Routing (BARS/NARS) software. By partitioning stations, TIE trunks, DISA DNs, and authorization codes into unique NCOS groups, you can track the normal calling patterns of each group (TFN002). You can then promptly detect variances which can indicate fraudulent activity, and take action.

Within the NCOS, you can assign the user to one of eight Facility Restriction Levels (FRL). The FRL is compared to the minimum FRL requirement assigned to each entry in a route list. The entries in the route list are trunk routes that are able to place calls to the NPA, NXX, or special number. The routes are listed in the order the system searches them when trying to complete an external call. Callers are eligible to complete a call on an entry in the route list when their FRL is equal to, or higher than, the entry's FRL level.

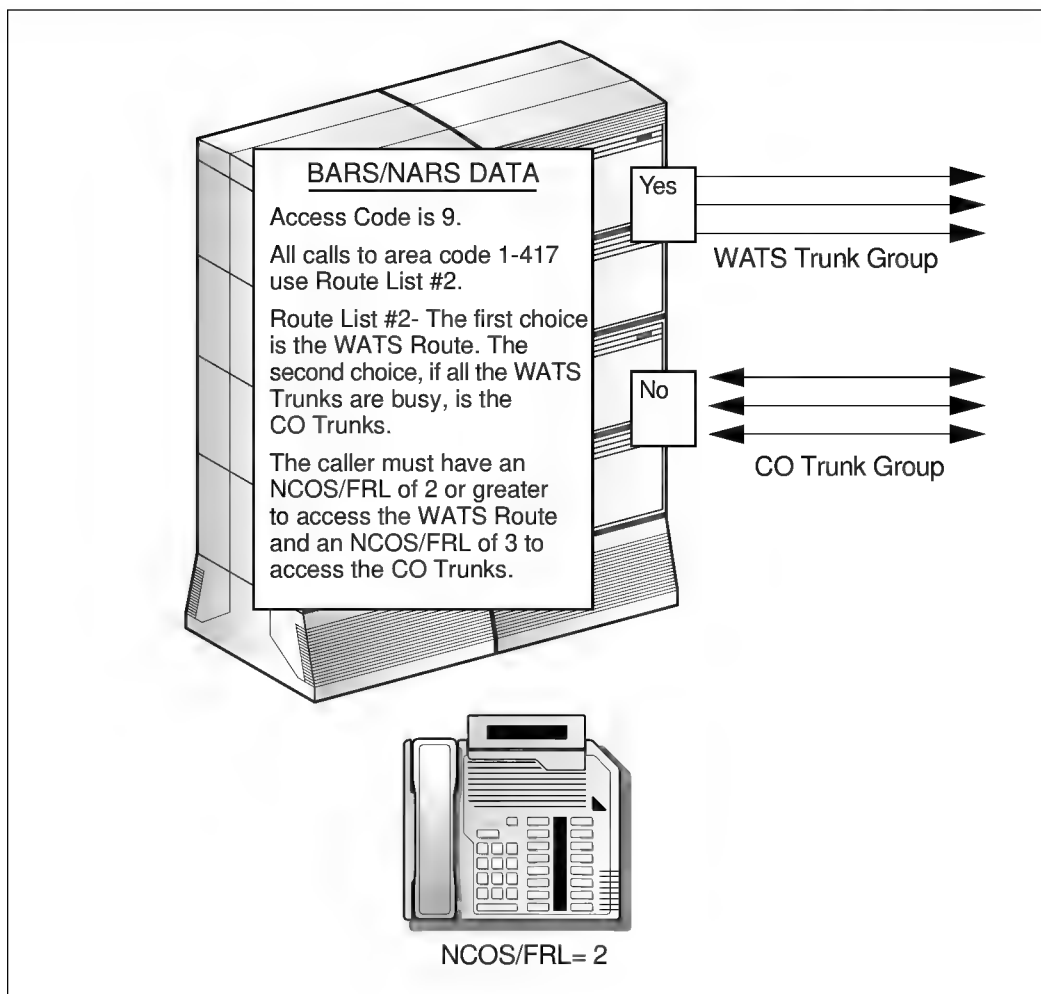
In conjunction with TGAR

The BARS/NARS database can be configured to ignore Trunk Group Access Restrictions (TGAR) or to use them. When TGARs are ignored, the BARS/NARS software assesses the Class of Service and the FRL to determine which call facilities are eligible for a particular call. This configuration allows flexibility in using a given trunk group while forcing users to place calls through BARS/NARS. You can base trunk access for each call on the FRL requirements for the number dialed rather than basing it on the TGAR.

You can also configure the BARS/NARS database to assess TGAR assignments in determining how the system can route a call. In this case, the BARS/NARS software will use the COS, TGAR, and FRL to determine which call facilities are eligible to process a particular call.

Example

The following illustration shows how the NCOS Facility Restriction Level feature works.



G100454

In this example, the following occurs:

- The user dials 9-1-417-555-9090.

Example, cont'd

- The 9 triggers the Option11C Compact to use BARS/NARS data.

- The Option11C Compact searches the Translation Table for 1417.
- Calls to 1417 use Route List Index 2.
- Route List Index 2 is searched for an idle available trunk.
- The first choice is the WATS route.
- The NCOS/FRL assigned to the first choice (2) is compared to the NCOS/FRL (2) of the station.
- The station's NCOS/FRL (2) is equal to, or greater than, the WATS NCOS/FRL (2), so the call is allowed for this choice.
- If all WATS trunks are busy, then the second choice (CO trunks) is checked.
- The NCOS/FRL of the CO trunks (3) is compared to the NCOS/FRL of the station (2).
- The station's NCOS/FRL (2) is lower than the CO trunks' NCOS/FRL (3), so the call cannot be completed over CO trunks.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the NCOS Facility Restriction Level feature.

For	Implement using	Print using
Network control	LD 87—NCTL all prompts	LD 87 FEAT=NCTL by NCOS
Route list index	LD 86—RLB, FRL	LD 86 FEAT=RLB
Authorization code	LD 88—AUT, NCOS	LD 88 TYPE=AUT
Stations	LD 10 and LD 11—NCOS	LD 10, 11 by TN LD 20 by TNB LD 81 by NCOS
Trunk	LD 14—NCOS	LD 20 by TNB

For	Implement using	Print using
Customer	LD 15—NCOS, FCNC	LD 21 by CDB or ESN/CDR
System Speed Call list	LD 18—NCOS	LD 20 by SCL
DISA	LD 24—NCOS	LD 24 by DISA DN

Network Speed Call

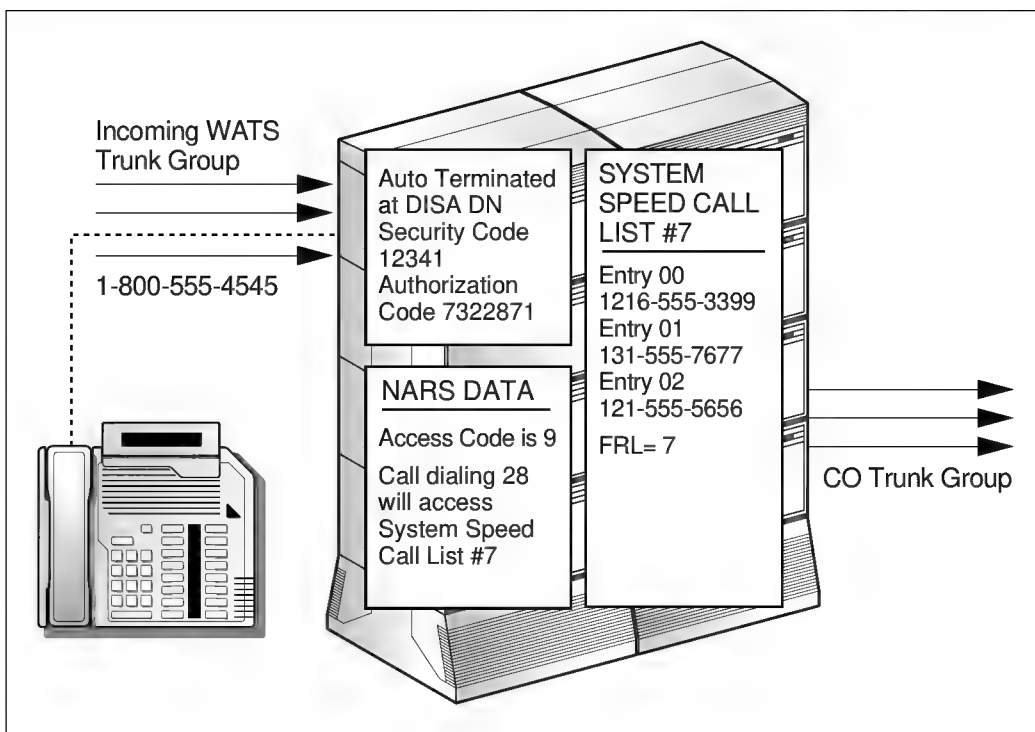
Description

You can enable a user who is normally restricted from making certain types of BARS/NARS calls, to make such a call if the destination is a company-approved number defined in a System Speed Call list. Network Speed Call expands the System Speed Call feature by allowing users to access the System Speed Call feature from the public and private networks.

You can use the Network Speed Call feature in conjunction with a restricted DISA DN. The incoming DISA caller can gain access to approved destinations through the Network Speed Call list.

Example

The following illustration shows how the Network Speed Call feature works.



G10045E

In this example, the following occurs:

- The caller dials 1-800-555-4545.
- When dial tone is returned, the user dials 12341.
- When dial tone is returned, the user dials 167322871
- When dial tone is returned, the user dials 9-28-00 to access System Speed Call Number 7.
- 9 triggers the Option1 IC Compact to use NARS data.
- the Option1 IC Compact checks the Translation Table for 28 and finds 00 to be the Access Code for System Speed Call List 7.

Example, cont'd

- System Speed Call List is checked for entry 00.
- The call completes to 1-216-555-3399 based on the calling capabilities of NCOS/FRL 7.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Network Speed Call feature.

For	Implement using	Print using
Network translation	LD 90—NSCL all prompts	LD 90 AC1 or AC2, SSCL
System Speed Call	LD 18—SSC all prompts	LD 20 by SCL
Network control	LD 87—NCTL, NSC, LIST	LD 87 by NCOS
Authorization code	LD 88—AUT, NCOS	LD 88 by AUT
Stations	LD 10 and LD 11—NCOS	LD 10, 11 by TN LD 20 by TNB LD 81 by NCOS
Trunk	LD 14—NCOS	LD 20 by TNB
Customer	DL 15—NCOS, FCNC	LD 21 by cdb or ESN/CDR
System Speed Call List	LD 18—NCOS	LD 20 by SCL
DISA	LD 24—NCOS	LD 24 by DISA DN

Network Authorization Code

Description

With the Network Authorization Code feature, you can assign up to 20,000 authorization codes of up to 14 digits each, and you have the options of requiring users to enter an authorization code before certain calls can be processed. You may want to use this requirement for certain locations typically associated with unauthorized access like the 809 area code.

Authorization Code Conditionally Last

Introduction

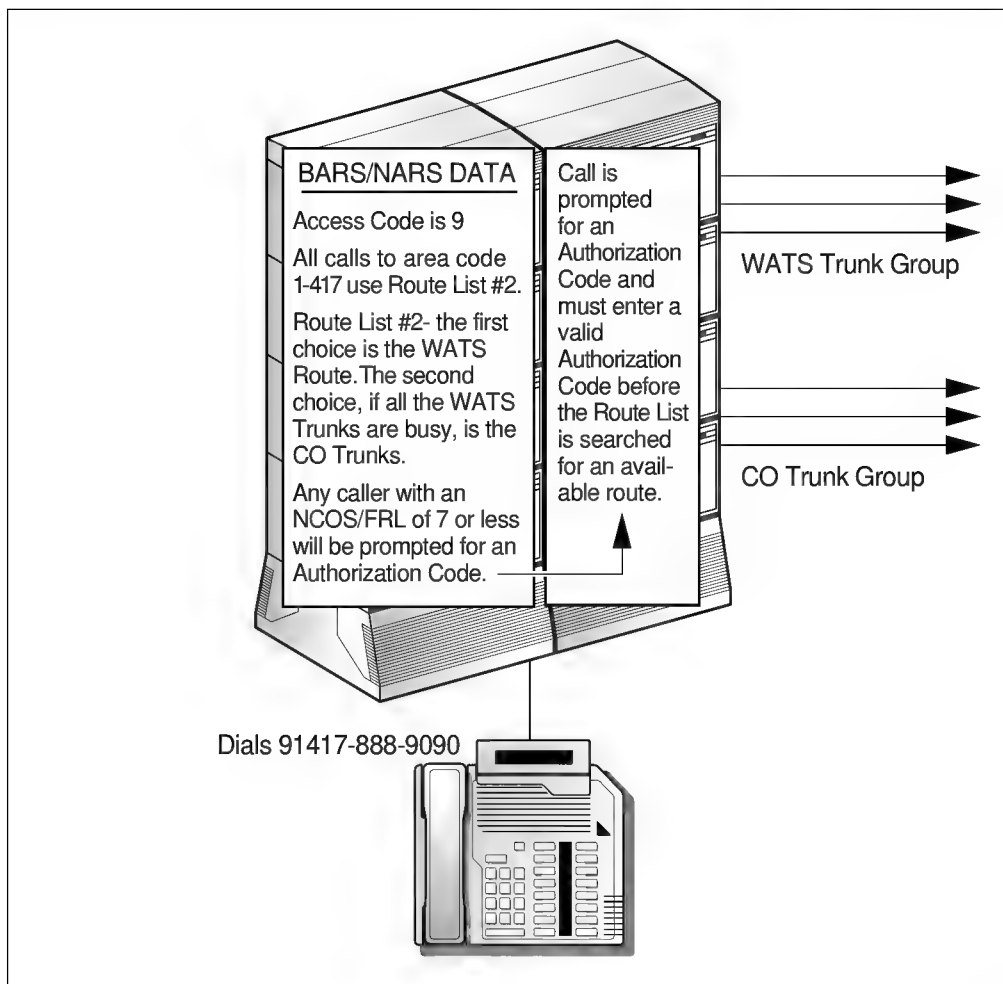
The system can prompt users “conditionally” for an authorization code after they attempt to place a call using the BARS/NARS call processing software. Users who fail to meet the minimum Facility Restriction Level requirement assigned to a route list will hear tones or a recorded announcement indicating that they need to enter an authorization code.

How this feature works

Users must enter a valid authorization code at that point to complete the call. This control provides another level of security by requiring all callers placing calls to international locations or selected area codes, for example, to enter an authorization code.

Example

The following illustration shows how the Authorization Code Conditionally Last feature works.



G100456

In this example, the following takes place:

- The user dials 9-1-417-555-3376.

Example, cont'd

- 9 triggers the Option11C Compact to use the BARS/NARS data.

- The Option 11C Compact checks the Translation Table for 1417 and sends calls to Route List Index 2.
- The system checks Route List Index 2 for the minimum NCOS/FRL required; it is found to be 7.
- The NCOS/FRL of 7 is compared to the user's NCOS/FRL, in this case 2.
- Because the user's NCOS/FRL is equal to or lower than the minimum NCOS/FRL for the route list, the user is prompted for an authorization code.
- The user must enter a valid authorization code before the call can be completed. The calling capabilities of the authorization code's NCOS/FRL will determine call eligibility.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Authorization Code Conditionally Last feature.

For	Implement using	Print using
Authorization code	LD 88—all prompts	LD 88 by AUT
Route List Index	LD 86—RLB MFRL	LD 86 by RLB
Network Control	LD 87 —NCTL, NCOS FRL	LD 87 by NCOS
Authorization Code	LD 88—AUT CODE, NCOS	LD 88=AUT
Stations	LD 10 and LD 11—NCOS	LD 10, 11 by TN LD 20 by TNB LD 81 by NCOS
Trunk	LD 14—NCOS	LD 20 by TNB
Customer	LD 15—NCOS, FCNC	LD 21 by CDB or ESN/CDR
System Speed Call List	LD 18—NCOS	LD 20 by SCL
DISA	LD 24—NCOS	LD 24 by DISA DN

Time-of-Day Routing

Description

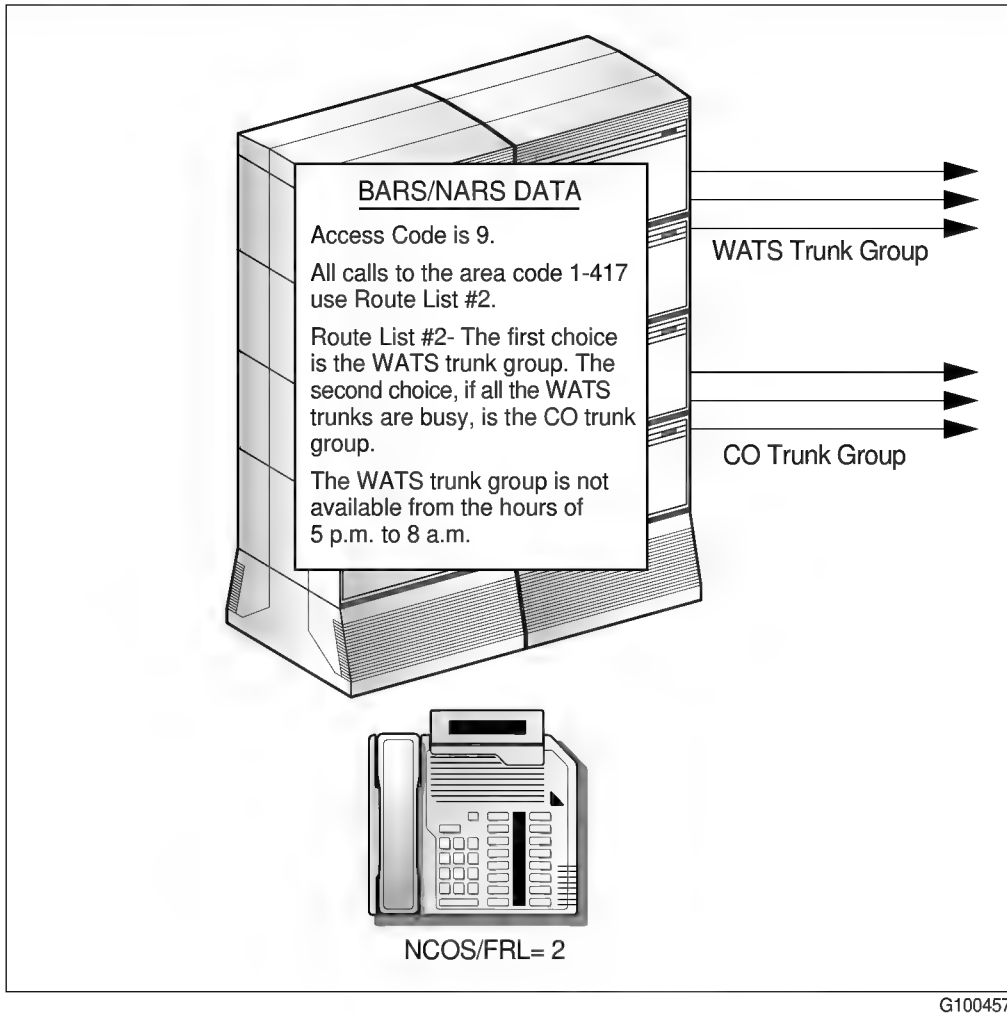
Time-of-day routing allows you to restrict access to certain destinations during specified time frames. For example, because the majority of fraudulent toll calls occur on holidays or after normal business hours, you can use this feature to turn off the route lists supporting calls to international locations or to the 809 area code after hours. Whether you can take this action depends on the needs of your users.

How this feature works

The Time-of-Day Routing feature specifies the hours that users can access each entry in a route list. BARS/NARS provides for up to eight time-of-day schedules. With this feature you can specify the most cost-effective route alternatives based on the time of day, and restrict employees from calling locations they have no need to call for business purposes at certain hours.

Example

The following illustration shows how the Time-of-Day Routing feature works.



In the example, the following occurs:

- The user dials 9-1-417-555-9090 at 6:00 p.m.

Example, cont'd

- 9 triggers the Option11C Compact software to use BARS/NARS data.

- The system checks the Translation Table.
- Calls to 1417 use Route List Index 2.
- The system searches Route List Index 2.
- The first choice, a WATS Route, is not available at 6:00 p.m.
- The second choice, CO Trunks, is available, and the call is sent out over the CO trunks.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Time-of-Day Routing feature.

For	Implement using	Print using
ESN	LD 87—ESN TODS	LD 87 by ESN
Route List Index	LD 86—RLB TOD	LD 86 by RLB

Routing Control

Introduction

Again, because the majority of toll fraud and internal abuse occurs after normal business hours, or on weekends or holidays, you may want to program the system to automatically modify users' calling privileges during these times.

Description

The Routing Control feature lets you reduce or raise a user's network access capabilities if necessary.

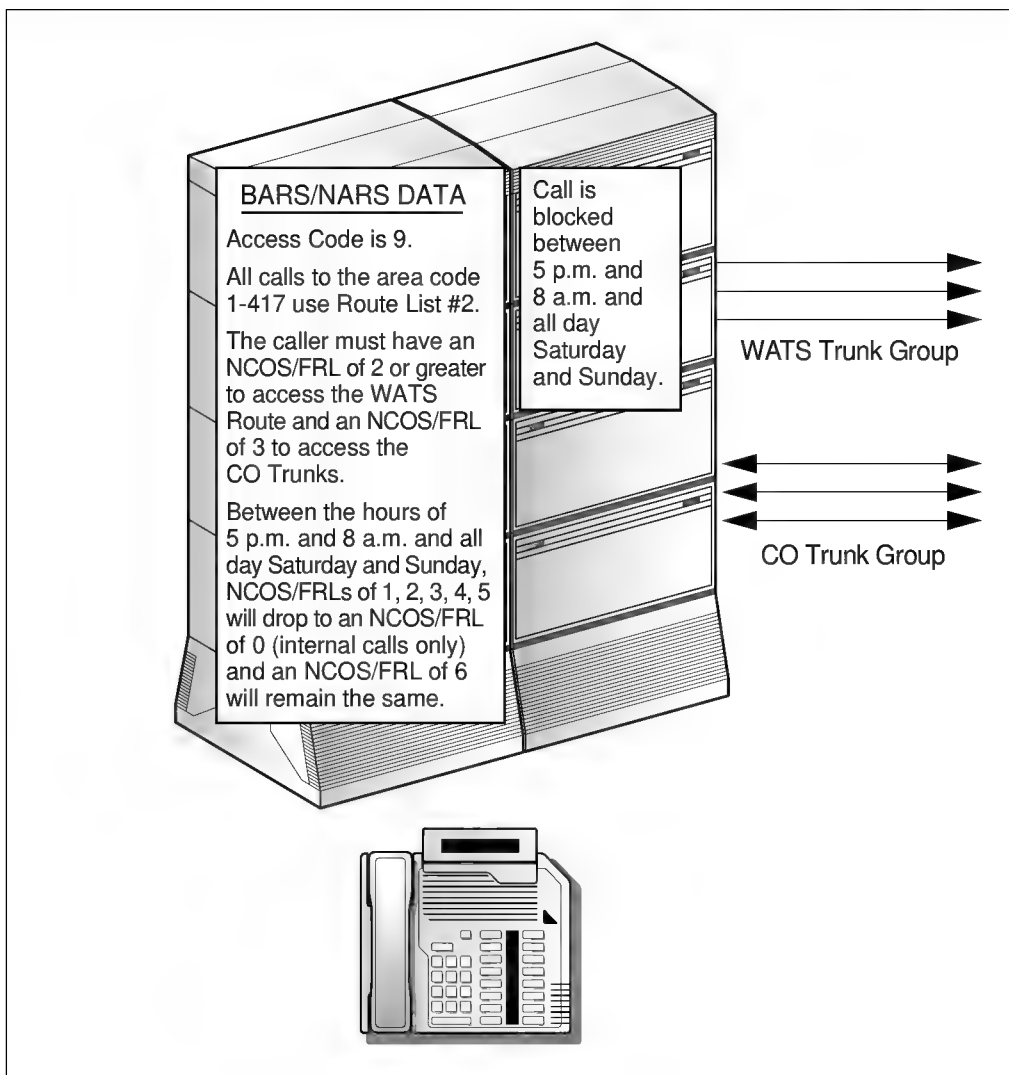
How Routing Control works

Each Network Class of Service (NCOS) is assigned an alternate NCOS when a special time-of-day schedule is in effect or during a specified day of the week. This feature enables you to change calling privileges automatically for a defined time frame each day or on weekends. You can also place a key on the attendant console that will manually activate routing control. With these features, you can implement controls on holidays and in response to critical situations.

Activating this feature prevents people from accessing unattended stations after hours to place unauthorized calls. However, authorization codes are not subject to the alternate NCOS assignments imposed through Routing Control. When users enter a valid authorization code, they are provided with the NCOS assigned to the authorization code for the duration of the call.

Example

The following illustration shows how the Routing Control feature works.



G100458

In this example, the following takes place:

Example, cont'd

- The user dials 9-1-417-555-4436 at 9:00 p.m.

- 9 triggers the Option11C Compact to use BARS/NARS data.
- Between 5:00 p.m. and 8:00 a.m., all users with an NCOS/FRL of 2 drop to an NCOS/FRL of 0.
- the Option11C Compact checks the Translation Table for 1417 and sends the call to Route List Index 2.
- A user must have an NCOS/FRL of 2 to access the WATS routes (first choice) and an NCOS/FRL of 3 to access the CO trunk group (second choice).
- Because it is between 5:00 p.m. and 8:00 a.m., the user's NCOS/FRL is 0.
- This call is not eligible for any route in the Route List Index.
- The call is blocked.

Implementing and auditing the feature

Use the following table to determine which overlay and prompts should be used to implement or audit the Time-of-Day Routing feature.

For	Implement using	Print using
ESN	LD 87—ESN, TODS 7, RTCL, NMAP ETOD	LD 87 ESN
Attendant	LD 12—KEY	LD 20 by TNB
Network Control	LD 87—NCTL NCOS	LD 87 by NCOS
Stations	LD 10 and LD 11—NCOS	LD 10, 11 by TN LD 20 by TNB LD 81 by NCOS
Trunk	LD 14—NCOS	LD 20 by TNB
Customer	LD 15—NCOS, FCNC	LD 21 by CDB or ESN/CDR
System Speed Call List	LD 18—NCOS	LD 20 by Speed Call List
DISA	LD 24—NCOS	LD 24 by DISA DN

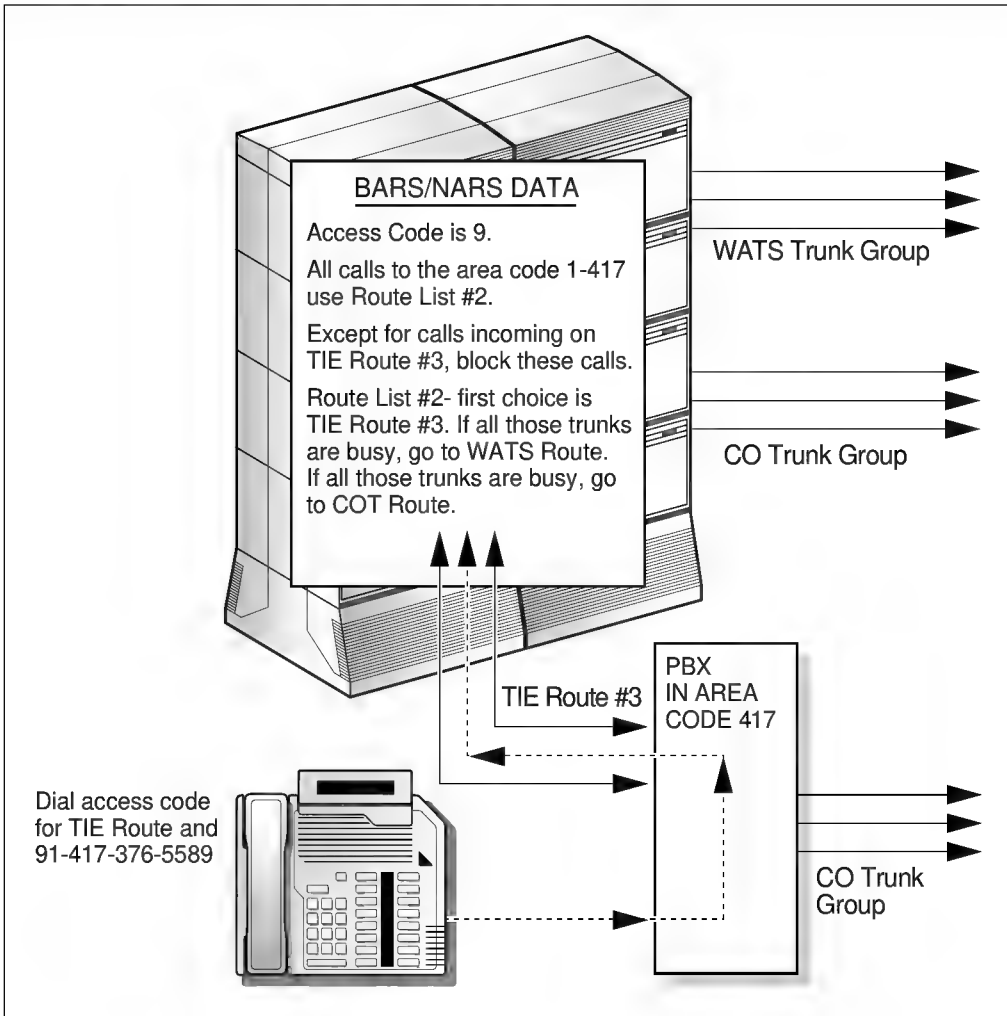
Incoming Trunk Group Exclusion

Description

You may want to control calls originating on various TIE routes. The Incoming Trunk Group Exclusion feature blocks BARS/NARS calls originating on TIE trunks from reaching destinations that employees do not need to reach for business purposes, and keeps users from attempting to circumvent the restrictions that are imposed at their home PBX. Each TIE route is associated with a table that defines the dialing sequences allowed for calls originated on that TIE route.

Example

The following figure illustrates how the Incoming Trunk Group (TIE) Exclusion feature works.



G100459

In this figure, the following occurs:

Example cont'd

- The user dials the access code for the TIE route and 9-1-417-555-5589.
- “9” triggers the Option11C Compact to use BARS/NARS data.
- BARS/NARS checks the Translation Table for the 417 area code and finds it restricted for calls from TIE Route 3.
- Option11C Compact validates that the call is incoming on TIE Route 3.
- The call is blocked.

Implementing and auditing the feature

Use the following table to determine which overlay and prompts should be used to implement or audit the Incoming Trunk Group Exclusion feature.

For	Implement using	Print using
ESN	LD 87—FEAT=ESN MXSD, MXIX	LD 87 FEAT=ESN
Incoming Trunk Group Exclusion	LD 86—FEAT=ITGE all prompts	LD 86 FEAT=ITGE by Incoming Trunk Group Exclusion Index
Network Translation	LD 90—FEAT=NET ITED, ITEI	LD 90 FEAT=NET by NPA or NXX or SPN

Section F **Controlling access to PBX administration programs**

In this section

<u>Overview</u>	<u>6-86</u>
<u>Password control</u>	<u>6-87</u>
<u>Limited access to overlays</u>	<u>6-89</u>
<u>Limited access password—user name</u>	<u>6-90</u>
<u>Multi-user login</u>	<u>6-91</u>
<u>Input/Output port recovery</u>	<u>6-92</u>
<u>History file</u>	<u>6-93</u>

Overview

Introduction

You can use the following to control access to PBX administration programs:

- Password control
 - Level 1 password
 - Level 2 password

For more information, [see “Password control” on page 6-87.](#)
- Limited access to overlays

For more information, [see “Limited access to overlays” on page 6-89.](#)
- Limited access password—user name

For more information, [see “Limited access password—user name” on page 6-90.](#)
- Multi-user login

For more information, [see “Multi-user login” on page 6-91.](#)
- Input/Output port recovery

For more information, [see “Input/Output port recovery” on page 6-92.](#)
- History file

For more information, [see “History file” on page 6-93.](#)

Password control

Introduction

Hackers have been known to access a system to obtain printouts of valid authorization codes, reassign control characteristics, defeat security measures in place, or degrade system performance. By controlling system passwords, you can minimize unauthorized access to the system. You can define a number of passwords that administrators can use to access the system for the purpose of the database.

Two types of passwords

Two types of passwords allow access to all aspects of the database and maintenance programs:

- Level 1 password
- Level 2 password

Level 1 password

You can use the Level 1 password to log on to the switch. Upon entering the valid password, you can change virtually all aspects of the database with the exception of changing the Level 1 and 2 passwords and, if defined, the secure data password associated with assigning authorization codes and DISA parameters.

Implementing and auditing the Level 1 password

Use the following table to determine which overlays and prompts should be used to implement or audit the Level 1 password.

For	Implement using	Print using
Configuration	LD 17—PWD2, NPW1	LD 22 by PWD

Level 2 password

The Level 2 password provides all the capabilities of the Level 1 password, and also allows you to change the Level 1 and Level 2 passwords as well as the secure data password as well as access to LPPW.

**Implementing and
auditing the Level 2
password**

Use the following table to determine which overlays and prompts should be used to implement or audit the Level 2 password.

For	Implement using	Print using
Configuration	LD 17—PWD2, NPW1	LD 22 by PWD

Limited access to overlays

Description

The Limited Access to Overlays (LAPW) feature provides a greater degree of control of password assignment and overlay access. In addition, it expands tracking of switch access.

This feature provides additional security by allowing you to define up to 100 LAPW passwords per system. The LAPW password may be 4 to 16 alphanumeric characters in both uppercase and lowercase. A maximum of four characters are allowed in either Password 1 or Password 2.

How LAPW works

You can define access to specific overlays for each password and specify a “Print-only” capability. You can also configure an audit trail to record the date, time, and password used, and the overlay programs accessed.

The system monitors failed logon attempts, compares the number with a predefined threshold, and locks the entry port if the threshold is exceeded. The Option11C Compact reports lock-out conditions on all TTYs and provides a special report to the next administrator who logs on.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Limited Access to Overlays feature.

For	Implement using	Print using
Configuration	LD 17—LAPW, PWNN, OVLY, CUST, TEN, OPT, LPWED, NLPW, FLTH, LOCK, AUDT, SIZE, INIT	LD 22 by CFN or LAPW

Limited access password—user name

Introduction In addition to Level 1 and Level 2 passwords and the 100 limited access passwords, the switch software can also require users to enter a user name with up to eight alphanumeric characters. Only the Level 2 password can configure user names, and change and print all passwords.

LAPW users may change their own passwords but not their user names.

Implementing and auditing the feature Use the following table to determine which overlays and prompts should be used to implement or audit the Limited Access Password feature.

For	Implement using	Print using
CFN	LD 17—LNAME_OPTION, LOGIN_NAME	LD 22 TYPE CFN, AUDT

Multi-user login

Description

Multi-user login allows up to three users to simultaneously log in to an Option11C Compact PBX to load and execute overlays. A fourth overlay running in the background or at midnight is also allowed.

The feature is activated and deactivated in Overlay 17.

Switch software support

The switch software supports only Set Administration (Overlays 10 and 11), associated print loads (Overlays 20, 21, and 22), Maintenance, Midnight Routines and Background Routines as re-entrant overlays.

Forced logoff

Additionally, a user can force the logoff from a specific terminal when logged in to Level Password 1 or 2 or an appropriate Limited Access Password.

Monitoring input/output

The monitor command allows a logged in user to monitor the input/output of a different specified terminal either locally or remotely; this feature is assigned on a per password level or to the Level 2 password.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Multi-user Login feature.

For	Implement using	Print using
CFN	LD 17—PWD2, LAPW, TLOG, SIZE, MULTI-USER, OPT	LD 22 PRT by CFN or LAPW

Input/Output port recovery

Introduction

Ports defined as TTY and PRT are controlled by two counters monitoring invalid characters. Ports disabled due to garbage characters or interference can be automatically enabled after a four-minute timer has expired.

Disabled ports can be enabled a maximum of three times in thirty minutes. The fourth time a port is disabled in a thirty-minute period requires manual enabling. Messages print at the TTY each time the port disables and reenables.

Implementing and auditing the feature

The feature is built into the base software.

No alteration is possible.

History file

Description

You may want to track certain system messages or activity and print that information at will. The History file stores system messages in memory. You can access the stored information through a system TTY or from a remote location, and you can print its contents.

How the History file works

You can specify the types of information that you want to store in the History file including maintenance messages (MTC), service change activity (SCH), customer service change activity (CSC), traffic outputs (TRF), and software error messages (ERR and BUG). By storing SCH activity and TRF output messages, you can store records of unauthorized access to the switch and retrieve information associated with calling patterns.

Using the VHST command

You may selectively view the History file using the command VHST. Commands allow you to search forward, repeat the last forward or backward search, and perform other various navigational movements within the file.

The History file may also have three categories of files: Log files ([see “Multi-user login” on page 6-91](#)), System History file, and Traffic files. Traffic files have two categories: system (scheduled) or user-generated reports. There is one traffic file per system.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the History file feature.

For	Implement using	Print using
Configuration	LD 17—HIST, ADAN, USER	LD 22 CFN or ADAN

Section G **Controlling Direct Inward System Access**

In this section

<u>Overview</u>	<u>6-96</u>
<u>DISA and security codes</u>	<u>6-97</u>
<u>DISA and Class of Service</u>	<u>6-98</u>
<u>DISA and authorization codes</u>	<u>6-99</u>

Overview

Description: DISA

Direct Inward System Access (DISA) provides a convenient means by which employees, when they are offsite, can place calls to internal extensions, and to private and public network locations by accessing your company's switching system.

How DISA is abused

The type of unauthorized access associated with this feature begins when perpetrators find the telephone number associated with DISA. In most DISA intrusion cases, hackers use PC-based programs to obtain valid DISA DNs, and security and authorization codes. Once a PC program finds a valid DISA telephone number, the PC inputs codes, redials the telephone number repeatedly, and stores the valid codes. Hackers then sell the numbers and codes they obtain illegally to third parties who then use this information for their own purposes.

In this section

In this section, you will learn how to effectively manage and monitor the Option 1 IC Compact's DISA feature.

DISA and security codes

Introduction

The first level of restricting DISA access is the security code.

How security codes work

If you program your system to require a security code, when the Option11C Compact answers a DISA call, callers must enter the security code assigned to the DISA DN before they can gain access to the system. This security code can be from one to eight digits long.

Remember, the longer the code, the harder it is for a hacker to crack.

DISA and Class of Service

Introduction

The second level of restriction is the class of service assigned to the DISA DN. Each DISA DN has its own Class of Service (COS), Trunk Group Access Restriction (TGAR), and Network Class of Service (NCOS).

How Class of Service works

When the Option11C Compact answers, if you do not require callers to enter authorization codes, then they automatically receive the DISA DN's calling privileges and class of service. You should consider making these controls as restrictive as possible (internal calls only, for example) and force users to enter an authorization code to access trunking facilities.

In addition, if the Option11C Compact records authorization codes in Call Detail Recording (CDR), you can track calls made through DISA and bill them back to users.

Implementing this feature

To implement this feature, [see "Class of Service" on page 6-13.](#)

DISA and authorization codes

Introduction

For a third level of security, you can require callers to enter an authorization code before they gain access to system facilities. You can assign authorization codes that are from 1 to 14 digits long. By assigning 14-digit authorization codes, you ensure that the hacker's PC-based code-cracking program has to try more combinations to obtain valid codes.

You can also configure Call Detail Recording to output the authorization codes used for call placement. In reviewing these reports, you should investigate any surge in activity for a given authorization code.

Assigning and changing codes

For further security, you should change authorization codes often and assign one code per person. If you cannot change authorization codes often because you have assigned a large number of codes and communicating the change would be difficult, then consider changing the DISA security code often.

Removal of codes

You should remove the authorization codes of terminated employees immediately. Establish a procedure with Human Resources or your Personnel department to advise you when employees leave the company.

Section H **Restriction/Permission lists**

In this section

<u>Overview</u>	<u>6-102</u>
<u>What are restriction/permission lists and codes?</u>	<u>6-103</u>
<u>Defaults</u>	<u>6-105</u>
<u>Understanding how restriction/permission codes work</u>	<u>6-106</u>
<u>Recommendations for using the first four restriction/permission lists</u>	<u>6-110</u>
<u>Defining and applying restriction/permission lists</u>	<u>6-111</u>

Overview

Introduction

In today's telecommunications environment, the same features that provide you with flexibility can also be the source of unauthorized use and abuse.

Meridian Mail Compact Option features

Features such as call answering/express messaging thru-dial, can dial numbers external to your telephone switch. This means that they can be used by users or external callers to place unauthorized long-distance calls at your organization's expense.

Restriction/permission lists

The primary weapon in your outcalling security arsenal are the restriction/permission lists. These lists are your first line of defense.

What are restriction/permission lists and codes?

Introduction

Restriction/permission lists are an important part of preventing users and callers from abusing your Meridian Mail Compact Option system.

Definition: restriction/permission list

A restriction/permission list is a group (or set) of restriction codes and permission dialing codes that can be applied to Meridian Mail Compact Option features or services that are capable of placing outcalls.

Up to 80 lists can be created, but each list must have a unique name. Each list can have up to 30 restriction codes and up to 30 permission codes. Once a list is defined, it can be applied to a number of Meridian Mail Compact Option features.

Definition: restriction code

A restriction code is a dialing code that Meridian Mail Compact Option is not permitted to dial. When Meridian Mail Compact Option is passed a number that begins with a restricted code, the call is blocked.

Restriction codes can be up to 20 digits in length.

Example 1

Your local dialing prefix is 9, your long distance dialing prefix is 91, and your international dialing prefix is 9011. You want to restrict all off-switch dialing. The restriction code is 9.

Example 2

Your long distance dialing prefix is 91 and you want to restrict calls to the 801 area code. The resulting restriction code is 91801.

**Definition:
permission code**

A permission code is a dialing code that Meridian Mail Compact Option is permitted to dial. These are usually exceptions to the restriction “rules.”

Permission codes can be up to 20 digits in length.

**Example of a
restriction/permission
list**

In this example 91 is the long distance dialing prefix and 9011 is the international dialing prefix. All internal extensions begin with 7 and 8.

List Name: Local

Restriction codes: 1 2 3 4 5 6 91 9011

Permission codes: 91617 911

This list restricts all international and long-distance calls, except those to 911 and to the 617 area code. In addition to the permitted codes, it allows on-switch calls to internal extensions beginning with 7 or 8, and local calls beginning with 9.

Defaults

Introduction

The defaults for new installations and conversions are described here. The default values when you first view a restriction/permission list are also described.

Defaults for new installations

For newly installed Meridian Mail Compact Option systems, all restriction/permission lists are fully restricted. The first four lists are named `On_Switch`, `Local`, `Long_distance_1`, and `Long_Distance_2`, and the remaining 76 lists are named `RPList5` to `RPList80` respectively.

ATTENTION

You must modify restriction/permission lists after installation. If you do not, many Meridian Mail Compact Option features that place outcalls will not work.

Default list entries

If you have not modified a restriction/permission list, it will be defined as follows the first time you view it:

Restriction codes: 0 1 2 3 4 5 6 7 8 9

Permission codes: (none)

Understanding how restriction/permission codes work

Introduction

The restriction codes in a restriction/permission list specify the general dialing rule. Permission codes are used to indicate any exceptions to the more general rules described by the restriction codes.

Levels of security

It is up to your organization to decide how to configure the restriction/permission lists. They are typically configured to provide various levels of security, from permitting only on-switch dialing (most secure) to allowing all long-distance dialing (least secure).

Examples

The following table contains examples of restriction/permission codes and how Meridian Mail Compact Option interprets them.

In these examples, 9 is the dialing code for local calls, and 91 is the dialing code for long distance calls.

Restriction code(s)	Permission code(s)	Result
91	91416, 9911	Most long-distance calls are restricted, except for 911 calls and numbers in the 416 area code.
1, 2, 5, 6, 7, 8, 9	none	All local and long distance calls are restricted. Internal extensions beginning with 3 or 4 are allowed.
91900	9	1-900 numbers are restricted, but local calls and all other long distance calls are permitted.

Rule

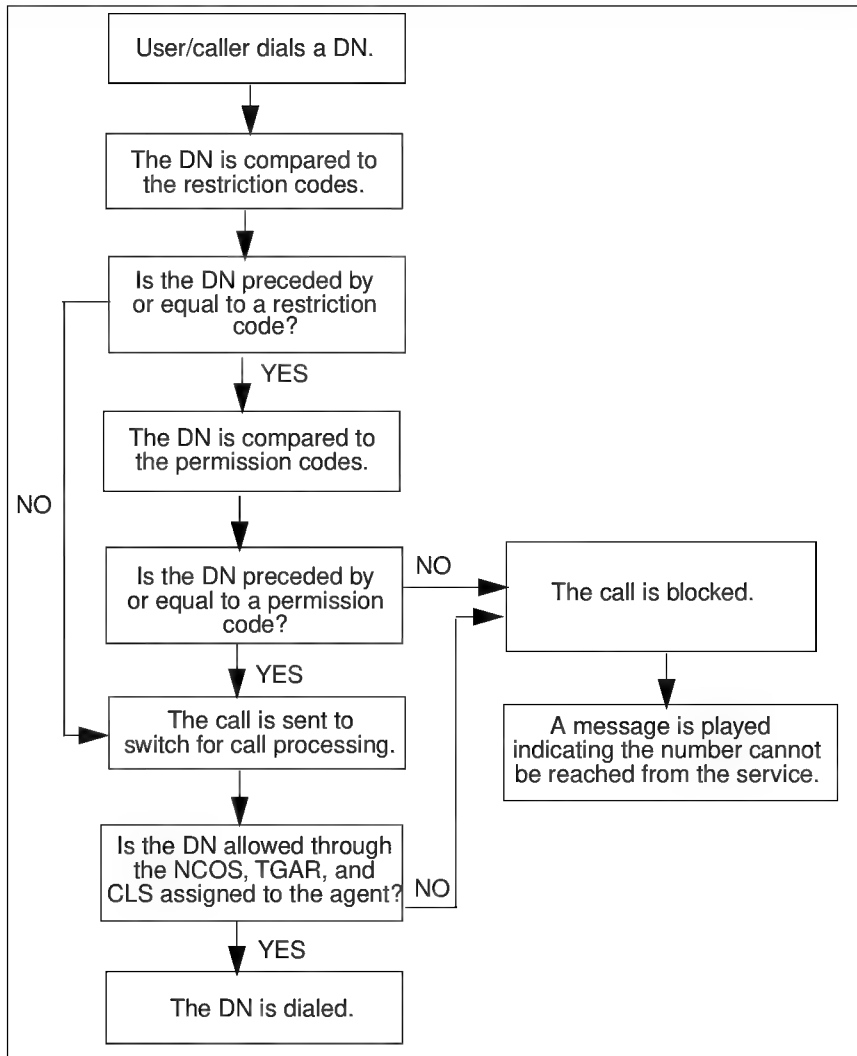
Numbers beginning with a permission code that is shorter than a restriction code and that matches a subset of the restriction code are allowed. They are not restricted.

Example

91900 is a restriction code. 9 is a permission code. Calls beginning with 9 (local calls) or 91 (long distance) are permitted as long as they are not beginning with 91900.

**How restriction/
permission codes are
processed**

The following flowchart shows how Meridian Mail Compact Option and the Meridian 1 process restriction and permission codes when a DN is dialed.

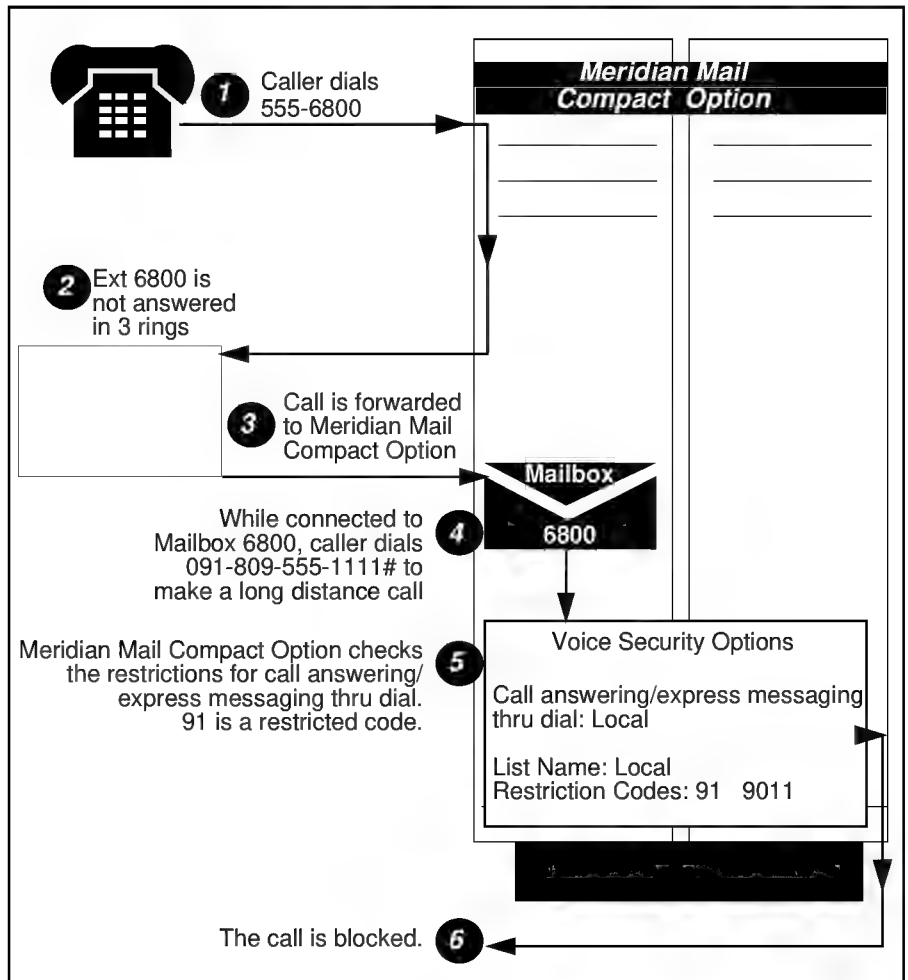


Example:
Call answering
thru-dial

Call answering/express messaging thru-dial allows callers to transfer to another internal extension or valid telephone number once Meridian Mail Compact Option answers. If

the proper restrictions are not placed on this feature, callers will be able to place calls at your organization's expense.

The following illustration shows how restriction/permission codes work in the case of call answering thru-dial.



Recommendations for using the first four restriction/permission lists

Introduction

The first four restriction/permission lists are named as follows:

- On_Switch
- Local
- Long_Distance_1
- Long_Distance_2

These names can be changed.

Recommendations

Nortel (Norther Telecom) recommends that you use the default restriction/permission lists as follows.

Note: You are responsible for developing a policy for restricting outcalling that is suitable to your organization's needs.

List name	List function	Restriction codes	Permission codes
On-switch	Permits calls to on-switch extensions only. Restricts all local, long distance, and international calls.	• local dialing prefix • long distance dialing prefix • international dialing prefix	optional (as required)
Local	Permits all on-switch and local calls. Restricts all long distance and international calls.	• long distance dialing prefix • international dialing prefix	optional (as required)

List name	List function	Restriction codes	Permission codes
Long Distance 1	Permits all on-switch calls, local calls, and long distance calls to certain area codes only. Restricts all international calls and long distance calls (in general).	• long distance dialing prefix • international dialing prefix	• specific long distance area codes
Long Distance 2	Permits all on-switch, local, and long distance calls. Restricts all international calls. or Permits all on-switch calls, local calls, and long distance calls to certain area codes only. (Similar in function to Long Distance 1, but permits different area codes.) Restricts all international calls and long distance calls (in general).	• international dialing prefix or • long distance dialing prefix • international dialing prefix • specific area codes	• none or • specific area codes

Defining and applying restriction/permission lists

Introduction

Restriction/permission lists can only be defined through the Restriction/Permission Lists screen. They are, however, applied to specific Meridian Mail Compact Option features or services through other screens.

Defining restriction/permission lists

To define restriction/permission lists, follow these steps.

Starting Point: The Main Menu

Step Action

- 1 Select Voice Administration.
- 2 Select Restriction/Permission Lists.
Result: The Restriction/Permission Lists screen appears.
- 3 Position the cursor beside the List number you want to view or modify.
- 4 Press the [SpaceBar] to highlight the list.
- 5 Press the [View/Modify] softkey.
Result: The View/Modify Restriction/Permission List screen appears.
- 6 Do you want to modify or view the codes in the list?

IF you want to**THEN**

modify the list

[go to step 7](#)

view the file

use the cursor keys to scroll through the screen and then
[go to step 10.](#)

- 7 Do you want to change the list name?

IF**THEN**

yes

press [Backspace] to delete the current name.

Enter the new list name.

no

[go to step 8.](#)

Step Action

8 Do you want to change the restriction codes?

IF

yes

THEN

delete the existing code (if not appropriate) and enter a new code.

Press <Return> or <Tab> to move to the next field.

Note: Repeat until all required restriction codes are either modified or added.

no

[go to step 9.](#)

9 Do you want to change the permission codes?

IF

yes

THEN

delete a code if required and enter the new code.

Press <Return> or <Tab> to move to the next field.

Note: Repeat until all required restriction codes are either modified or added.

no

[go to step 10.](#)

10 Do you want to save your changes?

IF

yes

THEN

press [Save].

no

press [Cancel].

Result: The Restriction/Permission Lists screen appears.

**Applying
restriction/permission
lists**

The following table identifies which Meridian Mail Compact Option screens are used to apply restriction/permission lists to Meridian Mail Compact Option features or services.

To apply restrictions/permissions to the following feature	Use the following screen
Call Answering/Express Messaging Thru-Dial	Voice Security Options
Extension dialing (mailbox thru-dial)	Add (or View/Modify) Class of Service
Custom Operator revert	
Thru-Dial service	Add (or View/Modify) Thru-Dial Definition

Section I **Controlling access to Meridian Mail Compact Option services and features**

In this section

<u>Overview</u>	<u>6-116</u>
<u>Custom Revert</u>	<u>6-118</u>
<u>Thru-Dial</u>	<u>6-122</u>
<u>Call Answering or Express Messaging</u>	<u>6-124</u>
<u>Extension dialing (mailbox thru-dial)</u>	<u>6-128</u>

Overview

Introduction

Meridian Mail Compact Option is a voice mail system that is integrated into the Meridian Mail Compact Option PBX. The system provides flexible features like Voice Menus which allow callers to choose from lists of services.

Restriction/ permission lists

You can minimize the risk of toll fraud and system abuse by using the restriction/permission features to control access to your Meridian Mail Compact Option system and switch. If you fail to put the proper safeguards in place, callers answered by your voice mail system can place toll calls.

Restriction/permission lists are applied to features that are capable of dialing outside your switch and are, therefore, a potential source of unauthorized system use and abuse.

Features to which restriction/permission lists can be applied

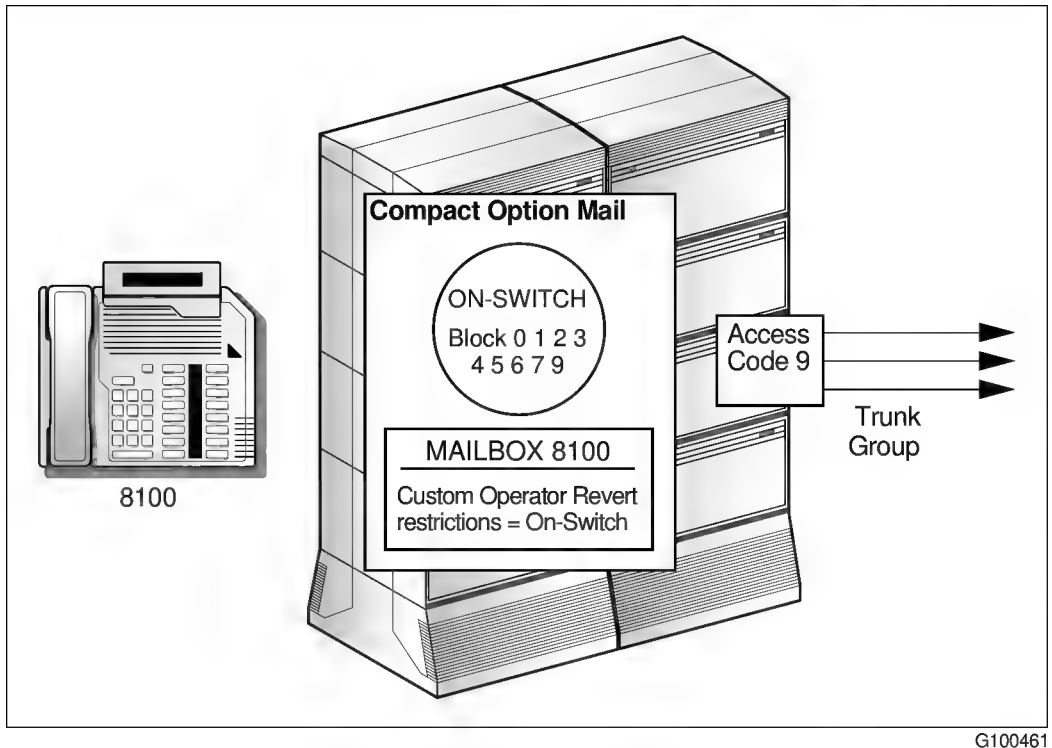
Restriction/permission lists can be applied to the following features.

Feature	Description
Custom (operator) revert	Users can define their own Custom Revert DN. Assign a list to this feature to restrict the DNs that users can specify.
Thru-dial services	Once connected to a thru-dial service, callers can thru-dial to external numbers if restrictions are not in place. Assign a list to all thru-dialers to restrict the numbers to which callers can thru-dial.

Feature	Description
Call answering/ Express messaging Thru-dial	Callers can transfer to other numbers during call answering and express messaging sessions. Assign a list to this feature to restrict the numbers to which callers are allowed to transfer themselves.
Extension dialing (mailbox thru-dial)	Users can thru-dial to other numbers while they are logged on to their mailbox. Assign a list to this feature to restrict the numbers to which they are allowed to thru-dial.
Call sender	Users can return a call with a single telephone set command (9). Assign a list to restrict the numbers they can call back with external call sender.

Custom Revert

Introduction	Once Meridian Mail Compact Option answers, callers may dial zero (0) anytime during the personal greeting or during the record cycle, and transfer to a predefined extension, usually a receptionist or secretary. This extension is the Revert DN.
Description	Each mailbox user can define his or her own Custom Revert DN through the telephone set. To prevent users from (unknowingly) abusing the system, you should assign restriction/permission lists to the revert feature.
Example	The following illustration shows how the Custom Operator Revert feature works.



G100461

Example, cont'd

In this example, the following takes place:

- The user logs in to Meridian Mail Compact Option.
- The user activates the Custom Operator Revert feature and attempts to define the operator revert as 9-555-0000.
- Meridian Mail Compact Option checks the Custom Operator Revert restrictions.
- The On-Switch Table blocks the code 9, and the function is disallowed.

Defining a restriction/permission list

To define a restriction/permission list, [see “Defining and applying restriction/permission lists” on page 6-111.](#)

Assigning a restriction/permission list

To assign a restriction/permission list to the Custom Revert feature, use the following procedure.

Step	Action
1	Log into the administration terminal.
2	Select Class of Service Administration from the Main Menu.
3	Press [View/Modify], and then enter the number of the class of service that the mailbox is using. If you do not know the class a. Press [Find]. b. Press [List]. c. Position the cursor beside the class you want to view or modify, and then press [SpaceBar] to highlight. d. Press [View/Modify]. Result: The Class of Service Administration screen for the particular class appears.

Step Action

- 4 Position the cursor beside the Custom Revert Restriction/Permission List field.
- 5 Enter the number of the restriction/permission list you want to assign to the Custom Revert feature.

Note: The name of the corresponding restriction/permission list does not appear until the cursor is off the field.

- 6 Do you want to save your changes?

IF	THEN press
yes	[Save].
no	[Cancel].

Thru-Dial

Introduction

All Thru-Dial services you create using the Voice Menus feature must be adequately protected with an appropriate restriction/permission list.

Defining a restriction/permission list

To define a restriction/permission list, [see “Defining and applying restriction/permission lists” on page 6-111.](#)

Assigning a restriction/permission list

To assign a restriction/permission list to the Thru-Dial service, use the following procedure.

Step	Action
------	--------

- | | |
|---|--|
| 1 | Log in to the administration terminal. |
| 2 | Select Voice Administration from the Main Menu. |
| 3 | Select Voice Services Administration from the Voice Administration menu. |
| 4 | Select Thru-Dial Definitions. |
| 5 | Position the cursor beside the definition, and press the [SpaceBar]. |
| 6 | Press [View/Modify]. |

Step Action

- 7 Position the cursor beside the Restriction/Permission List field.
- 8 Enter the number of the restriction/permission list you want to assign to the feature.

Note: The name of the corresponding restriction/permission list does not appear until the cursor is off the field.

- 9 Do you want to save your changes?

IF	THEN press
yes	[Save].
no	[Cancel].

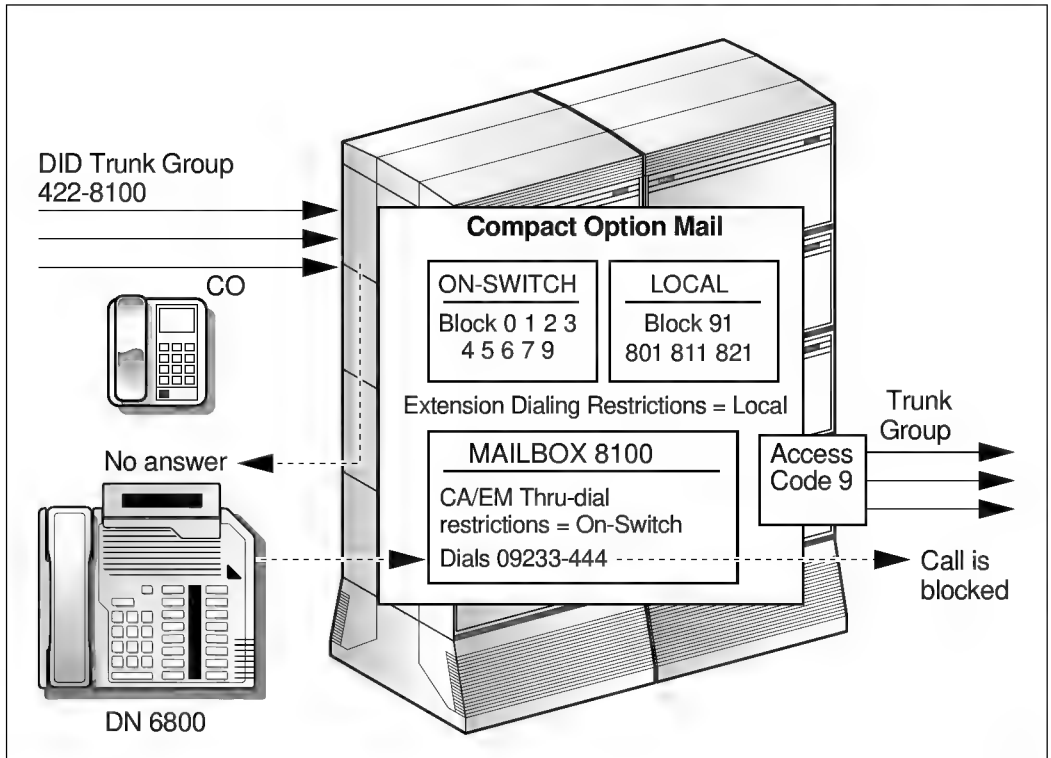
Call Answering or Express Messaging

Description

During a call answering or express messaging session, an external caller could potentially use thru-dial capabilities to place unauthorized calls which would be billed to the system. To use Thru-Dial, a caller must press 0 followed by a dialable DN. (If the caller waits more than two seconds after entering 0, he or she will be connected to an attendant instead.)

Example

The following illustration shows how the extension dialing feature works during a Call Answering/Express Messaging session.



G100462

Example, cont'd

In this example, the following takes place:

- The caller dials 555-8100. No answer is encountered at extension 8100.
- The caller is forwarded to Meridian Mail Compact.
- Once answered, the caller dials 09233-44.
- Meridian Mail Compact Option checks the Call Answering/Express Messaging Thru-dial restrictions.
- 9 is not allowed so the call is blocked. If the caller had logged in to Meridian Mail Compact Option, the call would have been allowed.

Restricting thru-dial capabilities

To prevent callers and users from abusing thru-dial capabilities during call answering or express messaging sessions, make sure an appropriate restriction/permission list is applied to call answering or express messaging thru-dial in the Voice Security Options screen.

To restrict thru-dial capabilities for call answering or express messaging sessions, use the following procedure.

Step Action

- 1 Select Voice Administration from the Main Menu.
- 2 Select Voice Security Options.

Step Action

- 3 Move the cursor to the Call Answering/Express Messaging Thru-Dial Restriction/Permission List Number field.
- 4 Enter the number of the restriction/permission list you want to apply to call answering and express messaging thru-dial.
Note: The name of the corresponding restriction/permission list does not appear until the cursor is moved off the field.
- 5 Do you want to save your changes?

IF**THEN press**

yes

[Save].

no

[Cancel].

Extension dialing (mailbox thru-dial)

Description

Another standard feature available with Meridian Mail Compact Option is extension dialing, or Thru-dial for mailboxes. The extension dialing feature allows callers to transfer to another extension number or valid telephone number once they log in to Meridian Mail Compact Option. Callers can dial zero (0) followed by an extension number, or valid access code, telephone number, and the pound sign (#).

Controls you can exercise

Meridian Mail Compact Option is shipped with the mailbox Thru-dial feature turned on. You can control access and use of Thru-dial in two ways:

- within the Meridian Mail Compact Option system
- within the Option 11C Compact system through the virtual agent

Controlling access within Meridian Mail Compact Option

This method allows you to define and apply the restrictions codes that best fit the needs of your user community and the security requirements of your organization.

This method involves

- defining restriction/permission lists
([see “Defining and applying restriction/permission lists” on page 6-111](#))
- applying restriction/permission lists to features

Note: [See “Applying a restriction/permission list” on page 6-129](#). These codes affect *all* mailbox Thru-dial functions that use the same Class of Service.

**Applying a restriction/
permission list**

To apply a restriction/permission list, use the following procedure.

Step Action

- 1 Log in to the administration terminal.
- 2 Select Class of Service Administration from the Main Menu.
- 3 Press [View/Modify], and then enter the number of the class of service that the mailbox is using.
If you do not know the class
 - a. Press [Find].
 - b. Press [List].
 - c. Position the cursor beside the class you want to view or modify, and then press [SpaceBar] to highlight.
 - d. Press [View/Modify].
- 4 Position the cursor beside the Extension Dialing Restriction/Permission List field.
- 5 Enter the number of the restriction/permission list you want to assign to the Extension dialing feature.
- 6 Do you want to save your changes?

IF	THEN press
yes	[Save].
no	[Cancel].

Controlling access within the switch

To control access of the Thru-dial feature within the Meridian Mail Compact Option PBX, use the following procedure. This method allows you to restrict the Thru-dial feature through the virtual agent.

Note: To restrict all access to the outside world through Thru-dial, be sure to restrict both your Least Cost Routing access code and your direct access code to each trunk group in the Option11C Compact.

Note: Be sure to block access to your Special Prefix (SPRE) code as well.

Step Action

-
- 1 Assign the appropriate Network Class of Service (NCOS).
For more information, [see "Network Class of Service—Facility Restriction Level" on page 6-63.](#)
 - 2 Assign the appropriate Trunk Group Access Restrictions (TGAR).
For more information, [see "Trunk Group Access Restrictions" on page 6-11.](#)
 - 3 Assign the appropriate Class of Service (COS).
For more information, [see "Class of Service" on page 6-13.](#)
-

The restrictions you impose through the virtual agent apply to Thru-dial functions accessed both through the voice menus feature and at the mailbox level.

Section J **Controlling access to Meridian Mail Compact Option mailboxes**

In this section

<u>Overview</u>	6-132
<u>Using the Voice Security Options screen</u>	6-134
<u>Default security settings</u>	6-141
<u>Initial password change</u>	6-143
<u>Password display suppression</u>	6-145
<u>Password prefix</u>	6-146
<u>Password length</u>	6-148
<u>Forced regular password changes</u>	6-149
<u>Invalid logon attempts</u>	6-153
<u>Modifying mailbox security settings</u>	6-157
<u>Restricting offsite access to mailboxes</u>	6-159
<u>Disabling unused mailboxes</u>	6-160

Overview

Introduction	Mailboxes are a potential source of unauthorized system use if proper safeguards are not put in place.
The kind of damage a hacker can do	The damage a hacker can do depends on what has been accessed: • A personal mailbox <i>without</i> thru-dial capabilities This causes minimal damage as the hacker has only gained access to the personal mailbox. In this case, the hacker would have access to all of the mailbox and message commands and could record obscene greetings, listen to messages, and so on. • A personal mailbox <i>with</i> thru-dial capabilities This can cause significant damage to your PBX and Meridian Mail Compact Option system especially if the hacker is able to break in to the system. • The business or Meridian Mail Compact Option system This can cause significant damage to your PBX and Meridian Mail Compact Option system since this mailbox usually allows users calling in access to the thru-dial feature.
Proactive mailbox security measures	Meridian Mail Compact Option provides four ways that you can control the level of security for users' mailboxes: 1. Use the password prefix and increase the minimum password length to make passwords harder to guess. 2. Force users to change their passwords regularly. 3. Control the number of maximum invalid logon attempts.

4. Disable external logon to mailboxes (when the highest level of security possible is required).

Using the Voice Security Options screen

Introduction

The Voice Security Options screen allows you to control various security features and set restriction and permission codes that can be applied to features such as call answering, call sender, Express Messaging, and mailbox Thru-Dial.

Voice Security Options screen

Part 1

This is the first part of the Voice Security Options screen.

Voice Administration	
Voice Security Options	
Password Prefix:	
Maximum Invalid Logon Attempts Permitted per session:	<u>3</u>
Maximum Invalid Logon Attempts Permitted per mailbox:	<u>9</u>
Maximum Days Permitted Between Password Changes:	<u>30</u>
Password Expiry Warning (days):	<u>5</u>
Minimum Number of Password Changes Before Repeats:	<u>5</u>
Minimum Password Length:	<u>4</u>
External Logon:	Enabled
More Below	
Select a softkey >	
Save	Cancel

Part 2

To view the additional fields in part 2 of the screen, press the <Page down> key or the down arrow.

Voice Administration		MORE ABOVE
Voice Security Options		
Call Answering/Express Messaging Thru_dial Restriction/Permission List Number:	2 Name: Local	
Force Password Change on Initial Logon:	No Yes	
Suppress Display of Telsat Password:	No Yes	
System Access Monitoring Period from (hh:mm):	23:00 to (hh:mm): 05:00	
Monitor All Thru-Dials during Monitoring Period:	No Yes Always_Monitor	
Monitor CLIDs during Monitoring Period:	No Yes Always_Monitor	
CLID Format	CLIDs to Monitor	
Internal:	_____	
MORE BELOW		
Select a softkey >		
Save	Cancel	

Field descriptions

The following fields are used to protect mailboxes against unauthorized use. The fields used to monitor mailbox access can be found in [Section K: Monitoring access to Meridian Mail Compact Option mailboxes and features](#).

Password Prefix

Description	The Password Prefix is a set of (up to four) digits that is inserted at the start of the default mailbox password whenever you create a new mailbox.
Default	System-generated four-digit code
Maximum Length	4 digits
	The prefix plus the user's DN cannot exceed 16 digits.

Maximum Invalid Logon Attempts Permitted per Session

Description	This is the maximum number of times a user or caller can enter an invalid password within one logon session.
Default	3
Valid Range	1 to 99

Maximum Invalid Logon Attempts Permitted per Mailbox

Description	This is the number of maximum invalid passwords that can be entered for a mailbox. This does not apply to the current logon session only. The number of invalid logons are counted over time.
Default	9
Valid Range	1 to 99

Maximum Days Permitted Between Password Changes

Description	This field determines how often users are forced to change their mailbox passwords.
Default	30
Valid Range	0 to 90 0 indicates users do not have to change passwords.

Password Expiry Warning (days)

Description	When a user's password is about to expire, a warning is played to notify the user and give him or her the chance to change it before it expires. This field determines how many days before password expiry the warning is played.
Default	5
Valid Range	0 to 60 0 indicates that a warning will not be played.

Dependencies	Displayed when the maximum days between password changes is 1 or greater.
--------------	---

Minimum Number of Password Changes Before Repeats

Description	This field determines the number of different passwords that must be used before the same password can be reused.
Default	5
Valid Range	0 to 5 0 indicates that users can reuse the same password.
Dependencies	Displayed when the maximum days between password changes is one or greater.

Minimum Password Length

Description	This is the minimum number of digits required in passwords that are entered from the telephone keypad. This includes mailbox passwords and access and update passwords for voice services.
Default	4
Valid Range	4 to 16

External Logon

Description	This feature is usually enabled to allow users to log on to their mailboxes from remote off-switch phones. This feature can be disabled to provide maximum security. When disabled, users cannot log on to their mailboxes from off-switch phones.
Default	Enabled

To disable	Call your Nortel distributor to disable this feature.
------------	---

ATTENTION

Once disabled, this feature can never be reenabled.

Valid Options	Enabled, Disabled
---------------	-------------------

Call Answering/Express Messaging Thru-Dial Restriction/Permission List Number

Description	This field indicates which Restriction/Permission List should be applied to Call Answering/Express Messaging Thru-Dials.
-------------	--

Default	2
---------	---

Force Password Change on Initial Logon

Description	This field compels users who are logging in to their mailbox for the first time to immediately change the default password.
-------------	---

Default	Yes
---------	-----

Suppress Display of Telset Password

Description	This field suppresses the display of password digits by replacing them with dashes on telephones with displays.
-------------	---

Default	Yes
---------	-----

Dependencies	None
--------------	------

System Access Monitoring Period from (hh:mm)

Description	This field indicates the monitoring period during which any or all of the following is monitored: • mailbox logons for requested users • the use of Thru-Dial services • the use of a mailbox or Thru-Dial service from a specified CLID
Default	Start time: 23:00 End time: 05:00

Monitor All Thru-Dials during Monitoring Period

Description	This field indicates whether all Thru-Dial services (from a mailbox, voice menu, or directly from a VSDN) are to be monitored, and if yes, when.
Default	No
Valid Options	No, Yes, Always_Monitor If Yes, you are prompted for the monitoring period.

Monitor CLIDs during Monitoring Period

Description	This field indicates whether calling line IDs (CLIDs) are to be monitored during logon or by the Thru-Dial service, and if yes, when.
Default	No
Valid Options	No, Yes, Always_Monitor If Yes, you are prompted for the monitoring period.

CLID Format—Internal—CLIDs to Monitor

Description	These are the internal CLIDs to be monitored during login or by the Thru-Dial service.
Default	None
Dependencies	The Monitor CLIDs during Monitoring Period field is set to Yes or Always_Monitor.

CLID Format—External—CLIDs to Monitor

Description	These are the external CLIDs to be monitored during login or by the Thru-Dial service.
Default	None
Dependencies	The Monitor CLIDs during Monitoring Period field is set to Yes or Always_Monitor.

Default security settings

Purpose

On a newly installed system, the security parameters are configured with default settings. These defaults may be appropriate for your system. If this is the case, you will not have to modify the settings.

However, the default settings may not adequately secure your Meridian Mail Compact Option system to meet your business requirements.

Security checklist

Review the checklist below to determine if you need to change any of the default values that are assigned to passwords. You can also fill in this checklist with your new settings.

Information about these parameters is provided on the following pages.

Parameter	Default value
Password Prefix	4-digit code
Maximum Invalid Logon Attempts Permitted per Mailbox	9
Maximum Invalid Logon Attempts Permitted per Session	3
Maximum Days Permitted Between Password Changes	30
Password Expiry Warning (days)	5
Minimum Number of Password Changes before Repeats	5
Minimum Password Length	4

Parameter	Default value
External Logon	Enabled
Call Answering/Express Messaging Thru-Dial Restriction/Permission List Number	2
Force Password Change on Initial Logon	Yes
Suppress Display of Telset Password	Yes
System Access Monitoring Period from (hh:mm)	23:00 to 05:00
Monitor All Thru-Dials during Monitoring Period	No
Monitor CLIDs during Monitoring Period	No
CLID Format—Internal—CLIDs to Monitor	None
CLID Format—External—CLIDs to Monitor	None

Initial password change

Introduction

Another measure to enhance security is to ensure that users change their initial password. This way, unauthorized access is prevented by those who may know the password prefix and mailbox number.

The initial password change feature provides the ability to force users to change their password the first time they log in.

How it works

When users log in to their mailbox for the first time, their default password is treated as “expired,” and they are forced to change their password at this time.

Note: When a user enters his or her password for the first time, and any time thereafter, it is not displayed on the telephone set display. For more information on this feature, see [“Password display suppression” on page 6-145](#).

Enforcing an initial password change

To ensure that new users are forced to change their passwords when they log in for the first time, use the following procedure.

Step Action

- 1 Select Voice Administration from the Main Menu.

Result: The Voice Administration menu appears.

Step	Action
------	--------

2	Select Voice Security Options.
---	--------------------------------

Result: The Voice Security Options screen appears.

3	Select Yes in the Force Password Change on Initial Logon field.
---	---

4	Do you want to save the configuration?
---	--

IF	THEN press
----	------------

yes	[Save].
-----	---------

no	[Cancel].
----	-----------

Password display suppression

Introduction

The password display suppression feature prevents display of entered password digits on telephone sets that have display screens. This prevents “shoulder surfers” from seeing your password.

How password display suppression works

When users enter their passwords, each digit in the password is replaced by a dash (-). The pound (#) key continues to be displayed as #, but the star (*) key is displayed as a dash if the feature is enabled.

This feature is not supported for external calls because the local switch has no control on the suppression capability.

Suppressing the display

To suppress the display of password each time a user logs in to Meridian Mail Compact Option, use the following procedure.

Starting Point: The Meridian Mail Main Menu

Step Action

1	Select Voice Administration. Result: The Voice Administration menu appears.
2	Select Voice Security Options. Result: The Voice Security Options screen appears.
3	Select Yes in the Suppress Display of Telset Password field.
4	Do you want to save the configuration?
IF	
THEN press	
yes	[Save].
no	[Cancel].

Password prefix

Introduction

When a new mailbox is created, the default password is the user's extension number. Until the user changes the default password, this may be a potentially serious security risk.

Password prefix

A password prefix provides another level of security by appending a short code before the default password. This code can be between two to four digits in length.

When a password prefix is defined, it is inserted at the beginning of the default mailbox password—the prefix is only inserted for new mailboxes.

Example

If mailbox 2339 is created and a password prefix of 34 has been defined, then the mailbox user will enter 342339 as the password the first time he or she logs in to Meridian Mail Compact Option.

How prefixes work

The password prefix only applies to new MMUI users regardless of whether it is being defined for the first time or has been changed.

The password prefix applies only until the user changes the password. For example, when the user of mailbox 2339 changes the password for the first time, the prefix is no longer required.

Guidelines

Change the password prefix on a regular basis for maximum security. When you change the password prefix, it does not affect existing mailboxes, only newly created mailboxes.

Setting up the password prefix

To apply a password prefix, use the following procedure.

Starting Point: The Meridian Mail Main Menu

Step Action

- 1 Select Voice Administration.
Result: The Voice Administration menu appears.
- 2 Select Voice Security Options.
Result: The Voice Security Options screen appears.
- 3 Enter the prefix in the Password Prefix field.
Note: The combined password prefix and the actual password cannot exceed 16 digits in length.
- 4 Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Password length

Introduction
The length of the password, in conjunction with other mailbox features, can make it very difficult for hackers to break into your Meridian Mail Compact Option system. You should never depend on one feature alone to safeguard your system.

How having a long password increases security
A long password increases your security provided that the password and the mailbox number are *not* the same. Having a long password means that there are more combinations to enter which could discourage the hacker.

Defining the password length
To define the minimum password length, use the following procedure.

Starting Point: The Meridian Mail Main Menu

Step	Action						
1	Select Voice Administration. Result: The Voice Administration screen appears.						
2	Select Voice Security Options. Result: The Voice Security Options screen appears.						
3	Set the password length in the Minimum Password Length field. Note: The password length including the password prefix cannot exceed 16 digits in length.						
4	Do you want to save the configuration?						
<table> <tr> <th>IF</th><th>THEN press</th></tr> <tr> <td>Yes</td><td>[Save].</td></tr> <tr> <td>No</td><td>[Cancel].</td></tr> </table>		IF	THEN press	Yes	[Save].	No	[Cancel].
IF	THEN press						
Yes	[Save].						
No	[Cancel].						

Forced regular password changes

Introduction

Forced password changes help increase security especially if they are done regularly. By compelling mailbox users to change their passwords and encouraging them to vary the length, it makes it very difficult for hackers to guess your password patterns.

Who can change the password

The mailbox password is changeable by both the administrator and the mailbox user. It can be altered as often as desired.

Relevant fields

The following fields in the Voice Security Options screen are related to forced password changes. The second and third fields are displayed only if the first field is set to a value of 1 or more:

- Maximum Days Permitted Between Password Changes
- Password Expiry Warning (days)
- Minimum Number of Password Changes before Repeats

For more information on the Voice Security Options screen and its fields, [see “Modifying mailbox security settings” on page 6-157.](#)

Maximum days between password changes

You can either force users to change their passwords on a regular basis, or you can allow them to change them when or if they want.

Default

On a newly installed system, the default setting forces users to change their passwords every 30 days. You can choose a value between 0 and 90 days.

Guideline

Forcing users to change their passwords on a regular basis is recommended since this results in a much greater level of security.

Expired passwords

If a user’s password expires, the user is not allowed to retrieve messages until he or she changes the password.

ATTENTION

If you change this value from 0 to another value on an operational system, user passwords expire immediately. Make this change during a slow traffic time and inform users of the change. After the change, you may notice a number of 3134 DR SEERs that indicate users did not change their passwords when prompted.

Password expiry warning

If the maximum days between password changes is set to 1 or more, you can play an expiry warning message to users before their password is about to expire. This warning reminds the user that the password is going to expire in X days and gives the user the chance to change the password before it expires.

This field gives you control over when this password is played.

WHEN this field is set to	THEN the warning will
a value between 1 and 60	be played this many days before the password is set to expire.

WHEN this field is set to	THEN the warning will
0	not be played. When the user's password expires, he or she will be prompted for a new password at logon.

Minimum password changes before repeats

To further increase mailbox security, you can force users to use a different password whenever their password expires. Otherwise, users may simply enter the same password over and over every time their password expires.

This setting is not applicable if the maximum days permitted between password changes is zero (0).

Enforcing regular password changes

To set up your system so that mailbox users will have to change their passwords, use the following procedure.

Starting Point: The Meridian Mail Main Menu

Step Action

- 1 Select Voice Administration.
Result: The Voice Administration menu screen appears.
- 2 Select Voice Security Options.
Result: The Voice Security Options screen appears.
- 3 Set the expiration period in the Maximum Days Permitted Between Password Changes field.
Note: The valid range is from 0 to 90 days and the default is 30. If you set this field to 0, the users are not forced to change their password and you do not have to configure any other fields. In this case, go to [step 6](#) to save or cancel the changes.

Step	Action
------	--------

- | | |
|---|--|
| 4 | Set the number of days of advance notice that users will hear before their password expires in the Password Expiry Warning (days) field. |
| 5 | Set the number of passwords that have to expire before a user can reuse an old password in the Minimum Number of Password Changes Before Repeat field. |
| 6 | Do you want to save the configuration? |

IF	THEN press
----	------------

yes	[Save].
no	[Cancel].

Invalid logon attempts

Introduction

The Invalid Logon Attempts feature allows you to define the number of times, within a range of one to nine, that a caller can enter an invalid logon password for a mailbox before the system disables the mailbox. Once the mailbox is disabled, only the system administrator can reenable it at the administration terminal. When a mailbox is disabled, Meridian Mail Compact Option still takes and stores incoming messages but does not permit logons.

The feature is useful in preventing hackers from entering one password after another until they gain access to a mailbox.

The feature also allows you to specify the number of invalid logon attempts per session as well as per mailbox. This discourages hackers from hopping around from one mailbox to another, disabling them with invalid logon attempts.

Relevant fields

There are two fields in the Voice Security Options screen that control the number of allowable invalid logon attempts:

- Maximum Invalid Logon Attempts Permitted per Session
- Maximum Invalid Logon Attempts Permitted per Mailbox

For more information on the Voice Security Options screen and its fields, [see “Modifying mailbox security settings” on page 6-157.](#)

Invalid logons per session

This field determines how many invalid passwords can be entered in a row during one logon session. If this limit is reached, the logon session is terminated.

Example

If a hacker knows your Meridian Mail Compact Option access code and some DNs, this is what would happen if your maximum invalid logon attempts per session were set to 3.

Attempt	Description
1	The hacker tries logging in to mailbox 2498 but enters an incorrect password.
2	The hacker tries logging in to mailbox 2498 again but enters an incorrect password.
3	The hacker tries logging in to mailbox 2475 but enters an incorrect password. The logon session is terminated.

Invalid logons per mailbox

Meridian Mail Compact Option also keeps track of how many invalid logon attempts have been made on each mailbox. This does not apply to the current logon session only. The number of invalid passwords entered is counted over time.

The counter is reset to 0 when the user changes the password.

If the limit is reached, the mailbox is disabled. Meridian Mail Compact Option still takes and records incoming messages, but does not allow the user to log on.

Disabling a mailbox

To specify how many invalid logon attempts will be allowed before a mailbox is disabled, use the following procedure.

Starting Point: The Meridian Mail Main Menu

Step Action

-
- | | |
|-----------|---|
| 1 | Select Voice Administration.
Result: The Voice Administration menu screen appears. |
| 2 | Select Voice Security Options.
Result: The Voice Security Options screen appears. |
| 3 | Set the number of invalid logon attempts per session in the Maximum Invalid Logon Attempts Permitted per Session field.
The valid range is from 1 to 99, and the default is 3. |
| 4 | Set the number of invalid logon attempts per mailbox in the Maximum Invalid Logon Attempts Permitted per Mailbox field.
The valid range is from 1 to 99, and the default is 9. |
| 5 | Do you want to save the configuration? |
| IF | THEN press |
| yes | [Save]. |
| no | [Cancel]. |
-

Reenabling a mailbox

To reenable a disabled mailbox, use the following procedure.

Starting Point: The Meridian Mail Main Menu

Step Action

-
- | | | | | | | | |
|-----------|---|-----------|-------------------|-----|--|----|---|
| 1 | Choose User Administration. | | | | | | |
| 2 | Choose Local Voice User. | | | | | | |
| 3 | Do you know the user's DN? | | | | | | |
| | <table border="0"><tr><td>IF</td><td>THEN</td></tr><tr><td>yes</td><td>press [View/Modify].
Enter the user's DN and
press <Return>.
Go to step 9</td></tr><tr><td>no</td><td>follow step 4 to step 8.</td></tr></table> | IF | THEN | yes | press [View/Modify].
Enter the user's DN and
press <Return>.
Go to step 9 | no | follow step 4 to step 8 . |
| IF | THEN | | | | | | |
| yes | press [View/Modify].
Enter the user's DN and
press <Return>.
Go to step 9 | | | | | | |
| no | follow step 4 to step 8 . | | | | | | |
| 4 | Press [Find] to do a search. | | | | | | |
| 5 | Specify the criteria for the search. | | | | | | |
| 6 | Press [List]. | | | | | | |
| 7 | Position the cursor beside the user you want to modify and
press the spacebar to highlight the entry. | | | | | | |
| 8 | Press [View/Modify] | | | | | | |
| 9 | Move the cursor to the Logon Status field. | | | | | | |
| 10 | Select Enabled. | | | | | | |
| 11 | Do you want to save the configuration? | | | | | | |
| | <table border="0"><tr><td>IF</td><td>THEN press</td></tr><tr><td>yes</td><td>[Save].</td></tr><tr><td>no</td><td>[Cancel].</td></tr></table> | IF | THEN press | yes | [Save]. | no | [Cancel]. |
| IF | THEN press | | | | | | |
| yes | [Save]. | | | | | | |
| no | [Cancel]. | | | | | | |
-

Modifying mailbox security settings

When to use

Follow this procedure

- after installation, if some or all of the default settings do not meet your organization's requirements
- to change the current settings to reflect a new security policy or tougher security measures

Procedure

To modify current mailbox security settings, use the following procedure.

Starting Point: The Meridian Mail Main Menu

Step	Action
------	--------

1	Select Voice Administration.
---	------------------------------

Step Action

- 2 Select Voice Security Options.
Result: The Voice Security Options screen appears.
- 3 Modify some or all of the following fields to meet your security requirements:
- Password Prefix
 - Maximum Invalid Logon Attempts Permitted per Session
 - Maximum Invalid Logon Attempts Permitted per Mailbox
 - Maximum Days Permitted Between Password Changes
 - Password Expiry Warning
 - Minimum Number of Password Changes before Repeats
 - Minimum Password Length
 - Force Password Change on Initial Logon
 - Suppress Display of Telset Password
- For more information, see the appropriate topics.
- 4 Do you want to save the configuration?
- | IF | THEN press |
|-----|------------|
| yes | [Save]. |
| no | [Cancel]. |
-

Restricting offsite access to mailboxes

Introduction

External logon is enabled by default, allowing users to log on to their mailboxes from phones that are external to the switch. If security is of the highest priority, Meridian Mail Compact Option provides a facility allowing the system to restrict access to a mailbox from an offsite location.

Implementing this feature

This feature (SW7007) can be ordered from a Nortel sales representative and is implemented by authorized field technicians.

ATTENTION

Once the external logon feature is disabled on the system, it can *never* be reenabled.

Disabling unused mailboxes

Introduction

Whenever employees are terminated, you should immediately disable their mailbox. This prevents them from abusing your system by billing toll calls to your company.

You should make arrangements with your personnel department to inform you of terminations so you can disable system access.

Procedure

To disable an unused mailbox, use the following procedure.

Starting Point: The Meridian Mail Main Menu

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select User Administration. |
| 2 | Select Local Voice User. |
| 3 | Press [View/Modify], and then enter the local voice user.
If you do not know the local voice user <ol style="list-style-type: none">Press the [Find] softkey followed by the [List] softkey.Position the cursor beside the user you want to view or modify, and press the [SpaceBar].Press [View/Modify]. |
| 4 | Position the cursor on the Logon Status field. |
| 5 | Set the field to Disabled to disable the mailbox. |
| 6 | Press [Save] to save the configuration. |
-

Section K **Monitoring access to Meridian Mail Compact Option mailboxes and features**

In this section

<u>Overview</u>	<u>6-162</u>
<u>Hacker Monitoring</u>	<u>6-163</u>
<u>Mailbox Login Monitoring</u>	<u>6-164</u>
<u>Thru-Dial Monitoring</u>	<u>6-166</u>
<u>CLID Monitoring</u>	<u>6-170</u>
<u>The Services Summary Traffic report</u>	<u>6-174</u>

Overview

Introduction

This section of the chapter describes the reports and features in Meridian Mail Compact Option intended to assist you in identifying attempts to violate the security of your system.

These include the following:

- the Services Summary Traffic report
- the Hacker Monitoring feature
- mailbox login monitoring
- Thru-Dial monitoring
- CLID monitoring

Hacker Monitoring

Introduction

This feature enables you to monitor selected or all mailbox logins and Thru-Dials, which helps you to check for activity on your system that may indicate the presence of hackers.

Description

The capability of hacker monitoring is provided by three different methods:

- by monitoring mailbox logins ([see “Mailbox Login Monitoring” on page 6-164](#))
- by monitoring the use of Thru-Dial services ([see “Thru-Dial Monitoring” on page 6-166](#))
- by monitoring mailbox logins or attempted Thru-Dials from specified calling line identification numbers (CLIDs) ([see “CLID Monitoring” on page 6-170](#))

Mailbox Login Monitoring

Introduction	Possible hacker activity may be detected by monitoring mailbox logins of requested local voice users.														
How to do it	You use the System Access Monitoring Period field on the Voice Security Options screen and the Monitor Mailbox during Monitoring Period field on the Local Voice User screen to set up mailbox login monitoring.														
Field descriptions	This table describes the fields that are used to set up mailbox monitoring. <table><tr><th colspan="2">System Access Monitoring Period</th></tr><tr><td>Description</td><td> This field indicates the monitoring period during which any or all of the following is monitored: • mailbox logins for requested users • the use of Thru-Dial services • the use of a mailbox or Thru-Dial service from a specified CLID </td></tr><tr><td>Default</td><td> Start time: 23:00 End time: 5:00 Both the start and the end time for this period are specified in the hh:mm format using the 24-hour clock. </td></tr><tr><th colspan="2">Monitor Mailbox during Monitoring Period</th></tr><tr><td>Description</td><td> When this field is set to Yes, all logins into the mailbox during the system access monitoring period will result in SEER 2262 being issued for MMUI users. </td></tr><tr><td>Default</td><td>No</td></tr><tr><td>References</td><td> For more information on local voice users, see Chapter 8, "Local voice users". </td></tr></table>	System Access Monitoring Period		Description	This field indicates the monitoring period during which any or all of the following is monitored: • mailbox logins for requested users • the use of Thru-Dial services • the use of a mailbox or Thru-Dial service from a specified CLID	Default	Start time: 23:00 End time: 5:00 Both the start and the end time for this period are specified in the hh:mm format using the 24-hour clock.	Monitor Mailbox during Monitoring Period		Description	When this field is set to Yes, all logins into the mailbox during the system access monitoring period will result in SEER 2262 being issued for MMUI users.	Default	No	References	For more information on local voice users, see Chapter 8, "Local voice users".
System Access Monitoring Period															
Description	This field indicates the monitoring period during which any or all of the following is monitored: • mailbox logins for requested users • the use of Thru-Dial services • the use of a mailbox or Thru-Dial service from a specified CLID														
Default	Start time: 23:00 End time: 5:00 Both the start and the end time for this period are specified in the hh:mm format using the 24-hour clock.														
Monitor Mailbox during Monitoring Period															
Description	When this field is set to Yes, all logins into the mailbox during the system access monitoring period will result in SEER 2262 being issued for MMUI users.														
Default	No														
References	For more information on local voice users, see Chapter 8, "Local voice users".														

Procedure

Use the following procedure to monitor mailbox logins.

Starting Point: The Meridian Mail Main Menu

Step Action

-
- | | |
|----|--|
| 1 | Select Voice Administration. |
| 2 | Select Voice Security Options. |
| 3 | Specify a time interval in the System Access Monitoring Period field. |
| 4 | Press [Save]. |
| 5 | Return to the Main Menu . |
| 6 | Select User Administration. |
| 7 | Select Local Voice Users. |
| 8 | Select the local voice user you want to modify or add.
For more information on modifying or adding local voice users, see Chapter 8, "Local voice users". |
| 9 | Set the Monitor Mailbox during Monitoring Period field to Yes. |
| 10 | Press [Save]. |
-

Thru-Dial Monitoring

Introduction

Possible hacker activity may be detected by monitoring selected or all Thru-Dial services used either during the system access monitoring period or at all times.

How to do it

Use the Voice Security Options screen and the Thru-Dial Definition screen to set up Thru-Dial Monitoring.

Note: The monitoring period is determined by the values entered in the System Access Monitoring Period from (hh:mm) field on the Voice Security Options screen.

IF you want to monitor	THEN in the Voice Security Options screen	AND in the Thru-Dial Definition screen
all Thru-Dials	set the Monitor all Thru-Dials during Monitoring Period field to Yes or Always_Monitor	no action is required.
specified Thru-Dials	set the Monitor all Thru-Dials during Monitoring Period field to No	for the desired service, set the Monitor this Service during Monitoring Period field to Yes.

Field descriptions

You will find descriptions of the Voice Security Options fields on page [6-134](#). For descriptions of the fields in the Thru-Dial Definition screen, see Chapter 25, "Class of Service administration".

**Field descriptions,
cont'd**

The following table only describes those fields which are used to set up Thru-Dial monitoring.

System Access Monitoring Period from (hh:mm)

Description	This field indicates the monitoring period during which one or all of the following will be monitored: • mailbox logons for requested users • the use of Thru-Dial services • the use of a mailbox or Thru-Dial service from a specified CLID
Default	Start time: 23:00 End time: 05:00
Available on	Voice Security Options screen

Monitor All Thru-Dials during Monitoring Period

Description	When this field is set to Yes, all accesses to the Thru-Dial service (from a mailbox, voice menu, or directly from a VSDN) during the system access monitoring period will result in a 10613 informational SEER. Included in this SEER is the CLID of the user. When this field is set to Always_Monitor, any access to the Thru-Dial service at any time will result in a class 106 informational SEER.
Default	No
Available on	Voice Security Options screen

Monitor this Service during Monitoring Period

Description	When this field is set to Yes, all accesses to this Thru-Dial service during the system access monitoring period will result in a 10613 informational SEER. Included in this SEER is the CLID of the user.
Default	No
Available on	Thru-Dial Definition screen

Monitoring all Thru-Dials

To monitor all Thru-Dials, use the following procedure.

Starting Point: The Meridian Mail Main Menu

Step Action

1	Select Voice Administration.						
2	Select Voice Security Options.						
3	Set the Monitor all Thru-Dials during Monitoring Period field to Yes or Always_Monitor.						
<table> <tr> <th>IF you have set this field to</th><th>THEN go to</th></tr> <tr> <td>Yes</td><td>step 4.</td></tr> <tr> <td>Always_Monitor</td><td>step 5.</td></tr> </table>		IF you have set this field to	THEN go to	Yes	step 4.	Always_Monitor	step 5.
IF you have set this field to	THEN go to						
Yes	step 4.						
Always_Monitor	step 5.						
4	Set the monitoring period in System Access Monitoring Period from (hh:mm) field.						
5	Press [Save].						

Monitoring specific Thru-Dials

To monitor a specific Thru-Dial, use the following procedure.

Starting Point: The Meridian Mail Main Menu

Step Action

-
- | | |
|---|--|
| 1 | Select Voice Administration. |
| 2 | Select Voice Security Options. |
| 3 | Set the Monitor all Thru-Dials during Monitoring Period field to No. |
| 4 | Set the monitoring period in System Access Monitoring Period from (hh:mm) field. |
| 5 | Press [Save]. |
| 6 | Go to the Thru-Dial Definitions screen. |
| 7 | Select the thru-dial definition you want to modify or add. |
| 8 | Set the Monitor this Service during Monitoring Period field to Yes. |
| 9 | Press [Save]. |
-

CLID Monitoring

Introduction

Possible hacker activity may be detected by monitoring mailbox logins or thru-dials that have been attempted from a specified calling line ID (CLID).

You can specify the type of CLID (Internal or External) and a string of digits (up to 15) of a CLID. That is, you can specify the complete CLID, the area code only, or the area code and office code. Up to twelve CLIDs can be entered for each type of CLID format. For more information on CLID, see Chapter 16, "Dialing translations".

How to do it

Use the Voice Security Options screen to set up CLID Monitoring.

IF you want to monitor	THEN in the Voice Security Options screen	AND in the Voice Security Options screen
CLIDs	set the Monitor CLIDs during Monitoring Period field to Yes or Always_Monitor	enter the numbers in the CLIDs to Monitor field.

Monitoring a subset of a CLID

If a subset of a CLID is to be monitored (an office code, for instance), this string of digits will be compared only to the beginning of the CLID and not with the number. Thus, if you want to monitor the office code, you must also specify the area code.

Field descriptions

The following table only describes those fields which are used to set up CLID monitoring. For descriptions of all the Voice Security Options fields, [see “Using the Voice Security Options screen” on page 6-134.](#)

Monitor CLIDs during Monitoring Period

Description	This field indicates whether CLIDs are to be monitored by the Voice Messaging Service during login or by the Thru-Dial service. This field also indicates when this monitoring should take place. When this field is set to No, CLIDs are not monitored, even if there are entries in the CLIDs to Monitor field. When this field is set to Yes, CLIDs are monitored during the system access monitoring period only. When this field is set to Always_Monitor, CLIDs are monitored at all times.
Default	No

CLIDs to Monitor

Description	You can enter up to 12 CLIDs. These CLIDs are monitored by Voice Messaging on mailbox login or by the Thru-Dial service if the Monitor CLIDs during Monitoring Period is set to Yes or Always_Monitor.
Maximum length	CLIDs can be up to 15 digits in length.
Format	You can enter complete CLIDs, area codes only, or area codes and office codes. Do not include any dialing prefixes, such as ESN prefixes, in the numbers you enter.

Examples	4165551234 is a complete CLID. 416 is an area code. All CLIDs from this area code are monitored. 416555 is an area code and exchange code. All CLIDs in the 555 exchange in the 416 area code are monitored.
Default	None

SEERs issued

An informational SEER is issued if the CLID of a caller matches one of the numbers specified in the Voice Security Options screen during a mailbox login or Thru-Dial access. The informational SEERs can be 5562, 2262, or 10612. For more information on SEERs, refer to the *Maintenance Messages (SEERs)* (NTP 555-7001-510).

Procedure

To monitor calling line IDs, use the following procedure.

Starting Point: The Meridian Mail Main Menu

Step Action

-
- | | |
|---|--|
| 1 | Select Voice Administration. |
| 2 | Select Voice Security Options. |
| 3 | Set the Monitor CLIDs during Monitoring Period field to Yes or Always_Monitor. |

IF you have set this field to**THEN go to**

- | | |
|----------------|-------------------------|
| Yes | step 4. |
| Always_Monitor | step 5. |
-
- | | |
|---|---|
| 4 | Set the monitoring period in the format hh:mm. |
| 5 | Enter the internal CLIDs to be monitored in the CLID Format—Internal block. |
| 6 | Enter the external CLIDs to be monitored in the CLID Format—External block. |
| 7 | Press [Save]. |
-

The Services Summary Traffic report

Introduction

This report provides statistics for each of the voice services installed on your system. It records the number of times a user dials a service (the number of accesses) during the reporting period and the average length of each access. The report records both direct and indirect accesses.

Direct accesses occur when a user dials the DN of the menu, or announcement.

Indirect accesses occur when a service is accessed from another service through a menu selection or a time-of-day controller.

For more information, see “Services Summary report” on page 30-12

Report availability

This report is available on all systems.

Report frequency

Run this report regularly to check for unusually long Thru-Dial sessions or for unusual numbers of after-hours Thru-Dial sessions. These may be a sign that hackers are present on your system.

What to do

If you suspect hackers are accessing the Thru-Dial feature, first check how the Thru-Dial service is set up to see whether the Operational Measurements (OM) data are unusual. For example, if executives call in and access a Thru-Dial service, then you can expect an average number of calls. If this average is exceeded, it may be an indication of hacker activity.

If your research still suggests the presence of hackers, review the dialing restrictions for Thru-Dial.

If you are using an access password for Thru-Dial, change the access password, and continue to monitor the Thru-Dial usage.

Section L **Equipment security**

In this section

<u>Overview</u>	<u>6-178</u>
<u>Switchroom access</u>	<u>6-179</u>
<u>Administration terminals</u>	<u>6-180</u>
<u>Meridian Mail Compact Option and switch printouts</u>	<u>6-182</u>

Overview

Introduction

This section of the chapter discusses security measures that you should exercise to safeguard the Meridian Mail Compact Option and switch hardware.

General security measures

The following is a list of general security measures you can take to secure your Meridian Mail Compact Option and Option 11C Compact switch:

- Limit access to your switchroom and escort all visitors.
- Keep a list of authorized technicians on hand. Whenever a regular technician appears, ask for ID to ensure that he or she is still employed by the company.
- Establish procedures for temporary technicians. Ask the technician for ID and to sign in, and issue a visitor's badge. If the technician does not have a company ID, check with the company to ensure that the person is a valid employee.

Switchroom access

Introduction

When a switchroom is not secure, criminals can gain access to all your system resources. Their activity can be as benign as turning off printers or as malicious as removing cards from your switch and rendering your system inoperable.

Security measures

The following is a list of safety measures you should exercise:

- Physically lock the room in which your equipment is located.
- Use combination locks—hardkey locks can easily be broken. Nortel recommends using an electronic key and program to safeguard your equipment room.
- Change the combination regularly and only inform those who need to know the new combination.

Administration terminals

Introduction

There are two facilities provided for protecting against unauthorized access to the Meridian Mail Compact Option administration terminal:

- the administration password
- hardware-based remote access restriction

Administration password

The administration terminal is password protected. When Meridian Mail Compact Option is first installed, there is a default password. The first time you log on to the Meridian Mail Compact Option administration terminal, you are forced to change this default password. You are recommended to change this password on a regular basis to maximize system security.

Passwords can be between 1 and 16 characters in length. However, it is recommended that the password be no less than seven characters in length. The longer the password, the less likely it is that someone will guess it.

Always log off before you leave the administration terminal, even if only for a short period.

Remote access restriction

If remote access is enabled on your system, anyone can dial in and commandeer your system. Remote access should not be enabled unless required (for example, for remote support personnel to work on your system).

Meridian Mail Compact Option systems are configured with an A/B switchbox between the terminal and the modem. When the switch is set to the modem setting, the system can be remotely accessed (but not from the local terminal). When the switch is set to the terminal setting, access is only

possible from the local terminal. The switch is controllable at the site and must be switched manually.

Meridian Mail Compact Option and switch printouts

Introduction

“Some man’s garbage is another man’s treasure.”

anonymous

This is very true for the telecommunication criminal known as the “dumpster diver.” These divers search through your garbage looking for printouts or records of your system’s codes.

Security measures

Do not throw out call detail records and credit card receipts. Dispose of these materials, including switch printouts and old documentation, as you do any proprietary materials.

Meridian Mail Compact Option

System Administration Guide

Toronto Information Products
Northern Telecom
522 University Avenue, 12th Floor
Toronto, Ontario M5G 1W7
Canada

© 1997
All rights reserved

Information is subject to change without notice.
Northern Telecom reserves the right to make changes
in design or components as progress in engineering
and manufacturing may warrant.

Meridian is a trademark of
Northern Telecom.

Publication number:	555-7001-333
Product release:	11
Document release:	Standard 1.0
Date:	November 1997

Printed in Canada

NORTEL
NORTHERN TELECOM